UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques
i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

El Teorema de Hasse-Minkowski

Autor: Joan Arnalot Farràs

Director: Dr. Xavier Guitart Morales
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 2 de juliol de 2020

Abstract

Hasse-Minkowski theorem states that a quadratic form has a non-trivial solution in $\mathbb{Q}$ if and only if there is a non-trivial solution in every completition. In this work we will study these completitions, their properties and their solutions in polynomials, the proof of the theorem and some applications and counterexamples in other polynomials than quadratic forms.

Resum

El teorema de Hasse-Minkoswki anuncia que una forma quadràtica té solució no trivial a $\mathbb{Q}$ si i només si en té a totes les seves completacions. En aquest treball estudiarem aquestes completacions, les seves propietats i l'existència de solucions en polinomis, la demostració del teorema i aplicacions i contraexemples d'aquest en polinomis que no siguin formes quadràtiques.

2010 Mathematics Subject Classification. 11-00

Agraïments

Per a l'Albert.

Índex

1 Introducció

Saber si una equació polinòmica té solucions racionals o no mai ha sigut senzill i és un problema obert per molts tipus d'equacions. Per el cas $x^2 + y^2 = -1$ sabem que no tenim solució en $\mathbb{Q}$ ja que no en té en la seva completació $\mathbb{R}$. Per tant si no en té en la seva completació llavors no en tindrà en el cos original. D'aquest cas en deriva una idea interessant que seria investigar si $\mathbb{Q}$ té més completacions i veure, anàlogament, quan no tenen solucions per així descartar cap possibilitat de solució racional.

En aquest treball veurem que els racionals només admeten certs tipus de normes: la trivial, la norma euclidiana i la p-àdica. Així , anàlogament a la construcció de $\mathbb{R}$ a partir de $\mathbb{Q}$ mitjançant la norma euclidiana, construirem els cossos p-àdics $\mathbb{Q}_p$ a partir de $\mathbb{Q}$ mitjançant la norma p-àdica.

Per tant, tot i que ja ho sabem, ara podríem deduir que $\sqrt{2}$ no és racional, ja que $x^2 - 2$ no té solució en $\mathbb{Q}_3$ i amb això ja sabem que no en pot tenir a $\mathbb{Q}$. Tot i que sí que en tingui en $\mathbb{Q}_7$.

Quan les equacions polinòmiques tenen solució i quan no en $\mathbb{Q}_p$ és un dubte raonable que resoldrem amb el lema de Hensel. Aquest demostra que és suficient amb trobar una aproximació en $\mathbb{Z}/p\mathbb{Z}$. En aquest cas anterior, 2 no és un quadrat en $\mathbb{Z}/3\mathbb{Z}$ però en canvi si que ho és en $\mathbb{Z}/7\mathbb{Z}$.

Però això no acaba aquí, ja que en aquest treball estudiarem el principi local-global introduït per Helmut Hasse. Aquest principi respon al fet que quan una propietat es compleix localment, llavors també ho fa globalment. El teorema de Hasse-Minkowski diu que aquest principi es compleix en les formes quadràtiques, o el que és el mateix, que si una forma quadràtica té solució no trivial a totes les completacions (compleix el requisit local), llavors aquesta mateixa forma quadràtica té solució en els racionals (resultat global).

La demostració no és senzilla i junt amb les eines que aquesta requereix hi destinarem la majoria del treball. Eines com les que ens proporcionarà l'estudi de les formes quadràtiques, de les que voldrem saber i sabrem quan tenen solució no trivial. Alhora que sabrem també quins elements representen les seves imatges, si són tots o només uns quants, o quan representen un determinat element.

Una altra eina molt útil és el símbol de Hilbert. Una aplicació binària $(a, b)_p$ que és igual a 1 quan $aX^2 + bY^2 - Z^2$ té solució no trivial i -1 quan no. Les propietats del símbol de Hilbert són bastantes. Una és el producte de Hilbert, que diu

$$\prod_{2 \leq p \leq \infty} (a, b)_p = 1,$$

on $p = \infty$ representa que estem avaluant-ho en el cos dels reals.

El símbol de Hilbert és molt present en tot el treball també en l'invariant de Hasse, que per una forma quadràtica $\phi = \alpha_1 X_1^2 + \alpha_2 X_2^2 + ... + \alpha_m X_m^2$ es defineix com:

$$c(\phi) = \prod_{1 \leq i < j \leq m} (\alpha_i, \alpha_j)_p.$$

i veurem que és invariant en formes equivalents.

El principi local-global no sempre es compleix, s'han trobat contraexemples per altres equacions polinòmiques. Un d'ells és el contraexemple de Selmer, $3X^3 + 4Y^3 + 5Z^3$, que mencionarem, i d'altres que veurem i demostrarem.

Per últim, analitzarem les aplicacions del teorema de Hasse-Minkowski. Aplicacions com la que demostra que un enter qualsevol pot ser expressat com a suma de 4 quadrats o 3 nombres triangulars.

Tot això ho farem seguint vàries referències en diferents apartats. Per la construcció dels nombres p-àdics hem seguit a Neal Koblitz en el seu llibre [1], així com per a l'estudi de les formes quadràtiques hem seguit a les notes de Yuri Bilu, [3]. Per a el símbol de Hilbert i els seus invariants, tant com per a la demostració en si i els seus contraexemples, hem seguit a Cohen en el seu llibre [4]. Per a les aplicacions i puntualment durant fragments del treball hem seguit a Serre en el seu llibre [2].

Estructura de la Memòria

En el primer capítol definirem els nombres p-àdics, abans de veure la seva construcció per així tenir una imatge mental d'on volem arribar. En el segon capítol ens aventurarem en la construcció d'aquest cos, definint primer la distància p-àdica i després completant el cos dels racionals mitjançant aquesta. Un cop definit i construït el cos p-àdic, n'estudiarem el comportament de les solucions en equacions polinòmiques, així com un cas concret sobre quan un nombre p-àdic és un quadrat o no.

En el tercer capítol farem un canvi sobtat de tema per estudiar les formes quadràtiques, molt presents en la resta del treball. Definirem les propietats d'universalitat, isotropia i regularitat, que ens permetran saber per exemple que a partir de 3 variables una forma quadràtica en un cos finit sempre té solució no trivial. Acabarem el tema aplicant els resultats a $\mathbb{Q}_p$.

Al quart capítol definirem el símbol de Hilbert i veurem el producte de Hilbert, que ens ajudaran a més a més a definir l'invariant de Hasse en el cinquè capítol per acabar demostrant el teorema de Hasse-Minkowski en el sisè capítol. El setè i el vuitè el dediquem a veure aplicacions i contraexemples del teorema i seguirem amb la conclusió on recapitularem breument el contingut matemàtic del treball.

Per finalitzar, tenim el capítol de context històric que ens proveirà d'una reflexió que inclou els protagonistes Helmut Hasse i Hermann Minkowski. Es basarà en les èpoques que van viure i com les van viure.

2 Nombres p-àdics

Hi ha vàries maneres de veure i entendre els nombres p-àdics. Fixant sempre un p primer es poden veure com un simple anell, on els elements son seqüències infinites d'elements en les que l'n-èssima coordenada pertany a $\mathbb{Z}/p^n\mathbb{Z}$ i tal que la mateixa seqüència $(b_1, b_2, b_3 \ldots, b_n, \ldots)$ compleix que per a tot n major que 1:

- $b_n \in \mathbb{Z}/p^n\mathbb{Z}$,
- $b_{n+1} \equiv b_n \pmod{p^n}$.

Per cada combinació d'aquestes tenim un element de $\mathbb{Z}_p$.
En el cas de $\mathbb{Z}_p$ diem que si $\phi(x)$ és el morfisme natural entre $\mathbb{Z}/p^{n+1}\mathbb{Z}$ i $\mathbb{Z}/p^n\mathbb{Z}$ que envia cada element de $\mathbb{Z}/p^{n+1}\mathbb{Z}$ al seu representant en $\mathbb{Z}/p^n\mathbb{Z}$, llavors $\mathbb{Z}_p$ és el límit projectiu $(\mathbb{Z}/p^n\mathbb{Z}, \phi_n(x))$.

La suma i el producte estan definits coordenada a coordenada, i són abelians, ja que $\mathbb{Z}_p$ és un subanell de $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$.
Veiem també que l'element neutre de la suma és el $0 = (0, 0, 0, \ldots)$ i l'$1 = (1, 1, 1, \ldots)$ en el producte. L'element invers respecte la suma de $(b_1, b_2, b_3, \ldots)$ és $(-b_1, -b_2, -b_3, \ldots)$. Per tant, tenim tots els ingredients per poder dir que $\mathbb{Z}_p$ és un anell.

També hi ha una notació que rep el nom d'expansió p-àdica, però per entendre-la primer hem de veure que si escollim la coordenada n-èssima b_n d'un element de $\mathbb{Z}_p$. Aquesta es pot expressar com $a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1}p^{n-1}$ on tots els coeficients a_i pertanyen a $\{0, 1, \ldots, p-1\}$. Bàsicament ens estem quedant amb el representant de b_n comprés entre 0 i p^n escrit en base p.
Veiem a més que si expressem de la mateixa manera b_{n+1}, com que aquest és congruent amb b_n en mòdul p^n els primers n coeficients són els mateixos. I així obtenim l'expansió p-àdica, que no és més que un altre tipus de notació, i que per $a \in \mathbb{Z}_p$, li assigna

$$a = \sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \ldots,$$

que en cap cas és un sumatori real amb un valor total, sinó una expansió finita o infinita.

Es pot canviar fàcilment d'una notació a l'altra usant senzilles operacions.
Per passar de l'expansió p-àdica a la coordenada n-èssima hem de fer la suma parcial fins a l'n-èssim element:

$$a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots \mapsto (a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots, \sum_{i=0}^{n} a_i p^i, \ldots)$$

En canvi, inversament, necessitem assegurar-nos que dins les nostres coordenades hem escollit els representants compresos entre 0 i $p^n - 1$, ja que sinó el resultat obtingut no compleix els requisits de l'expansió p-àdica.
Per fer-ho, calculem la diferència entre l'n-èssim component i el seu anterior. Com que són congruents en modul p^n, la seva diferencia és pot dividir per p^n i així obtenim el

factor n-èssim de l'expansió p-àdica. I repetim un altre cop que per fer aquest canvi és necessari que el representant de cada coordenada sigui el enter comprés entre 0 i $p^n - 1$.

$$(b_0, b_1, b_2, \ldots, b_n, \ldots) \longmapsto b_0 + (\frac{b_1 - b_0}{p})p + (\frac{b_2 - b_1}{p^2})p^2 + \ldots + (\frac{b_n - b_{n-1}}{p^n})p^n + \ldots$$

Cada tipus de notació ens pot ser útil per coses diferents. Generalment farem servir l'expansió p-àdica, ja que ens serà més útil per entendre $\mathbb{Q}_p$; el cos de fraccions de $\mathbb{Z}_p$. Val la pena saber que encara podríem fer ús de més tipus diferents de notació, com per exemple la notació que utilitza els representats "Teichmüller". Tenen també la forma $a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots$, però a_i en comptes de pertànyer a $\{0, 1, \ldots, p-1\}$, pertany al conjunt d'arrels en $\mathbb{Z}_p$ del polinomi $x^p - x$.

Seguint amb l'expansió p-àdica, el producte aquí és una mica més complicat. En el fons és molt semblant a la manera de multiplicar manualment però aquest cop d'esquerra a dreta. Aquí tenim un exemple de multiplicar $(3 + 6 \cdot 7 + 2 \cdot 7^2 + ...) \in \mathbb{Q}_7$ per $(4 + 5 \cdot 7 + 1 \cdot 7^2 + ...) \in \mathbb{Q}_7$:

$$\begin{array}{r}
3 + 6 \times 7 + 2 \times 7^2 + \cdots \\
\times\ 4 + 5 \times 7 + 1 \times 7^2 + \cdots \\
\hline
5 + 4 \times 7 + 4 \times 7^2 + \cdots \\
1 \times 7 + 4 \times 7^2 + \cdots \\
3 \times 7^2 + \cdots \\
\hline
5 + 5 \times 7 + 4 \times 7^2 + \cdots
\end{array}$$

Figura 1: Producte

Sigui amb la notació que sigui ara ens podríem preguntar quins elements de $\mathbb{Z}_p$ tenen inversa, i aquesta pregunta ens porta a la següent proposició:

Proposició 2.1. *Un element de $\mathbb{Z}_p$ és invertible si i només si no és divisible per p.*

Demostració. Recordem que p té la forma $p = 0 + 1 \cdot p$, per tant és obvi que si p divideix un element, aquest tindrà com a primer coeficient també 0. Així doncs, no serà invertible.

Per altra banda, veiem que si p no divideix l'element, aquest té inversa, on simplement cada element n-èssim de la inversa és la inversa de l'element n-èssim. Òbviament, això fa que el seu producte sigui 1, però encara hem de veure que les coordenades siguin congruents entre elles.

$$a_{n+1} \equiv a_n \pmod{p^n} \Leftrightarrow a_{n+1} a_{n+1}^{-1} a_n^{-1} \equiv a_n a_n^{-1} a_{n+1}^{-1} (mod p^n) \Leftrightarrow a_n^{-1} \equiv a_{n+1}^{-1} (mod p^n)$$

Per últim sabem que totes les inverses estan ben definides, ja que un element de A_n és invertible si i només si no és divisible per p. A més sabem que a_n no són divisibles per p ja que, del contrari, $a_n \equiv 0 \pmod{p}$ i això implicaria $a_0 = 0$, per tant, que p divideix l'element. Però això contradiu l'hipòtesi. □

Com hem dit al iniciar el capítol, aquesta és una manera potser una mica simple de mirar els nombres p-àdics; veure'ls com un anell, ja que també poden ser vists com una completació de $\mathbb{Q}$ respecte a una distància d. Una completació de $\mathbb{Q}$ similar a la que dona com a conjunt final $\mathbb{R}$ usant la distància euclidiana.

3 Construcció de $\mathbb{Q}_p$

La construcció de $\mathbb{Q}_p$ és molt similar a la construcció de $\mathbb{R}$ partint de $\mathbb{Q}$. Definim una distància que anomenarem distància p-àdica, completem $\mathbb{Q}$ respecte la distancia p-àdica amb els límits de successions d'elements p-àdics i acabem veient que totes les successions tenen un representant dins de $\mathbb{Q}_p$ i viceversa.

3.1 Distància p-àdica

Definició 3.1. *Si $\mathbb{X}$ és un conjunt no buit, una distància d és una funció que envia un parell (x, y) d'elements de $\mathbb{X}$ a un nombre real positiu tal que:*

$d(x, y) = 0$ *si i només si* $x = y$;
$d(x, y) = d(y, x)$ *per a tot* $(x, y) \in \mathbb{X}^2$;
$d(x, y) \leq d(x, z) + d(z, y)$ *per a tot* $z \in \mathbb{X}$.

Definició 3.2. *Una norma $\|\cdot\|$ és una aplicació d'un conjunt no buit $\mathbb{X}$ a els reals positius tal que:*

$\|x\| = 0$ *si i només si* $x = 0$
$\|x \cdot y\| = \|x\| \cdot \|y\|$ *per a tot* $x \in \mathbb{X}$
$\|x + y\| \leq \|x\| + \|y\|$ *per a tot* $(x, y) \in \mathbb{X}$

Proposició 3.3. *Si $\|\cdot\|$ compleix els requisits per ser norma, l'aplicació d que envia un parell d'elements de $\mathbb{X}^2$ a $\mathbb{R}$ definida per $d(x, y) = \|x - y\|$ és una distància.*

Demostració. Veiem que $\|1\| = 1$ i $\| - 1\| = 1$ per acabar veient que la simetria i la desigualtat triangular.

$$\begin{aligned} \|y\| = \|1 \cdot y\| = \|1\| \cdot \|y\| &\Leftrightarrow \|1\| = 1; \\ 1 = \|1\| = \|(-1) \cdot (-1)\| = \| - 1\|^2 &\Leftrightarrow \| - 1\| = 1; \\ d(x, y) = \|x - y\| = \| - (x - y)\| = \|y - x\| &= d(y, x); \\ d(x, y) = \|x - y\| = \|x - z + z - y\| \leq \|x - z\| + \|z - y\| &= d(x, z) + d(z, y). \end{aligned}$$

□

Definició 3.4. *Diem que una norma $\|\cdot\|$ intueix una distància d si $d(x, y) = \|x - y\|$.*

Exemple 3.5. Una norma a $\mathbb{Q}$ és el valor absolut $|x|$

$$|x| = \begin{cases} x, & \text{si x} \geq 0, \\ -x, & \text{si x} < 0 \end{cases}$$

Definició 3.6. *Sigui p un nombre primer i sigui a un enter, $ord_p(a)$ és el nombre de vegades que p divideix a. Si x és un nombre racional $x = \frac{a}{b}$,llavors l'ordre està definit per $ord_p(x) = ord_p(a) - ord_p(b)$. Concordem que $ord_p(0) = \infty$ per qualsevol p.*

Per a i b enters l'ordre del seu producte segueix una propietat semblant al logaritme: El nombre de vegades que p divideix ab és equivalent al nombre de vegades que p divideix a sumat al nombre de vegades que p divideix b. Al ser p primer, això fa que $ord_p(ab) = ord_p(a) + ord_p(b)$. A la vegada això demostra que qualsevol fracció equivalent a x té el mateix valor per la funció ord_p, ja que:

$$ord_p(\frac{ac}{bc}) = ord_p(ac) - ord_p(bc) = ord_p(a) + ord_p(c) - ord_p(c) - ord_p(b)$$
$$= ord_p(a) - ord_p(b) = ord_p(\frac{a}{b}).$$

Ara veiem que siguin a, b enters, els podem expressar com $a = p^{n_a} \cdot a'$ i $b = p^{n_b} \cdot b'$ on a', b' tenen ordre p-àdic 0. Llavors, si suposem que $\min\{n_a, n_b\}$ és n_a, tenim que $a+b = p^{\min\{n_a,n_b\}} \cdot (a' + b'p^{n_b-n_a})$, i veiem que l'ordre de $(a' + b'p^{n_b-n_a})$ és 0, ja que mòdul p és diferent de 0, el que provoca que $ord_p(a+b) = \min\{ord_p(a), ord_p(b)\}$. Ampliem això als racionals i veiem que:

$$ord_p(\frac{a}{b} + \frac{c}{d}) = ord_p(\frac{ad+bc}{bd}) = ord_p(ad+bc) - ord_pbd$$
$$= \min\{ord_pad, ord_pbc\} - ord_pbd = \min\{ord_pad - ord_pbd, ord_pbc - ord_pbd\}$$
$$= \min\{ord_p(\frac{ad}{bd}), ord_p(\frac{bc}{bd})\} = \min\{ord_p(\frac{a}{b}), ord_p(\frac{c}{d})\}.$$

Per tant, per tot x, y racionals la funció ord_p compleix:

$ord_p(xy) = ord_p(x) + ord_p(y)$;
$ord_p(x+y) = \min\{ord_p(x), ord_p(y)\}$.

Exemple 3.7. $ord_p(1) = 0$, $ord_5(5) = 1$, $ord_7(21) = 1$, $ord_3(54) = 3$, $ord_p(p^n) = n$, $ord_7(\frac{5}{3}) = 0$, $ord_{11}(\frac{1}{22}) = -1$, $ord_5(25/27) = 2$.

Definició 3.8. *La norma p-àdica per $x \in \mathbb{Q}$ és $\|x\|_p = p^{-ord(x)}$.*

Proposició 3.9. *$\|\cdot\|_p$ és una norma.*

Demostració. És obvi que $\|\cdot\|_p$ sempre és positiu. Veiem doncs que

$$\|xy\|_p = p^{-ord_p(xy)} = p^{-ord_p(x)-ord_p(y)} = p^{-ord_p(x)} \cdot p^{-ord_p(y)} = \|x\|_p \cdot \|y\|_p,$$
$$\|x+y\| = p^{-ord_p(x+y)} \leq p^{-\min\{ord_p(x),ord_p(y)\}} = \max\{p^{-ord_p(x)}, p^{-ord_p(y)}\}$$
$$= \max\{\|x\|_p, \|y\|_p\} \leq \|x\|_p + \|y\|_p.$$

□

Definició 3.10. *Una norma no-arquimediana és aquella que $\|x+y\| \leq \max\{\|x\|, \|y\|\}$ per a tot parell (x, y) del seu domini. Una norma arquimediana és una norma que no és no-arquimediana.*

Observació 3.11. La norma $\|\cdot\|_p$ és no-arquimediana.

Observació 3.12. Tots els triangles amb la norma $\|\cdot\|_p$ són isòsceles, ja que si $\|x\|_p \geq \|y\|_p$ llavors $\|x-y\|_p = \max\{\|x\|_p, \|y\|_p\} = \|x\|_p$. De fet és fàcil veure que amb qualsevol norma no-arquimediana també succeeix això.

Definició 3.13. *La norma trivial és aquella que*

$$\|x\| = \begin{cases} 0, & \text{si } x = 0, \\ 1, & \text{la resta de casos.} \end{cases}$$

Ara estem a punt de veure la "naturalitat"de la norma $\|\cdot\|_p$. Comprovarem que no hi ha gaires normes més en $\mathbb{Q}$ per tant el fet d'estudiar $\|\cdot\|_p$ i els conjunts que forma pren molt sentit.

Teorema 3.14. *(Ostrowski). Tota norma no-trivial $\|\cdot\|$ a $\mathbb{Q}$ és equivalent a $\|\cdot\|_p$ per algun p primer o a $|\cdot|$, el valor absolut.*

Demostració. Primer de tot hem de dir que una norma és equivalent a una altra si les successions que son de Cauchy en una norma també ho són en l'altra i viceversa. Sabem també que això succeeix si i només si $\|\cdot\|_1 = (\|\cdot\|_2)^\alpha$.
Seguim doncs amb la demostració i la dividim en dos casos:

Primer cas: Suposem que existeix un enter positiu n tal que $\|n\| > 1$. Escollim l'enter positiu més petit que compleixi això i l'anomenem n_0. Per tant, tenim un $\alpha \in \mathbb{R} > 0$ per el qual $\|n_0\| = n_0^\alpha$. Ara escrivim qualsevol enter positiu n en base n_0. Volem veure que $\|n\| \leq n^\alpha$.

$$\begin{aligned} n = a_0 + a_1 \cdot n_0 + a_2 \cdot n_0^2 + \ldots + a_m \cdot n_0^m, a_n \in (0, 1, \ldots, n_0 - 1), a_m > 0, \\ \|n\| \leq \|a_0\| + \|a_1 \cdot n_0\| + \|a_2 \cdot n_0^2\| + \ldots + \|a_m \cdot n_0^m\|, \\ = \|a_0\| + \|a_1\| \cdot \|n_0\| + \|a_2\| \cdot \|n_0\|^2 + \ldots + \|a_m\| \cdot \|n_0\|^m. \end{aligned}$$

Al ser tots els coeficients menors que n_0 tenen norma inferior o igual a 1. Per tant :

$$\|n\| \leq 1 + n_0^\alpha + n_0^{2\alpha} + \ldots + n_0^{m\alpha} = n_0^{m\alpha} \cdot (1 + n_0^{-\alpha} + n_0^{-2\alpha} + \ldots + n_0^{-m\alpha}),$$

Veiem que $n_0^{m\alpha} \leq n^\alpha$, ja que $n_0^m \leq n$, per tant, resumint:

$$\|n\| \leq n^\alpha \cdot \sum_{i=0}^{\infty} n_0^{-i\alpha} = C \cdot n^\alpha,$$

on C és una constant major que 1. Si ho avaluem en n^N en comptes de n tenim que $\|n^N\| \leq C \cdot n^{N\alpha}$ que és equivalent a $\|n\| \leq C^{1/N} \cdot n^\alpha$.
Si escollim N infinitament gran acabem veient que $\|n\| \leq n^\alpha$.

Seguint amb el primer cas ara volem veure que $\|n\| \geq n^\alpha$.

Partim de que $n_0^{m+1} > n \geq n_0^m$ per la descomposició de n en base n_0. Llavors:

$$\begin{aligned} \|n_0^{m+1}\| = \|n + n_0^{m+1} - n\| \leq \|n\| + \|n_0^{m+1} - n\|, \\ \Leftrightarrow \|n\| \geq \|n_0^{m+1}\| - \|n_0^{m+1} - n\|. \end{aligned}$$

Com que sabem que $\|n\| \leq n^\alpha$, llavors $\|n_0^{m+1} - n\| \leq (n_0^{m+1} - n)^\alpha$, així doncs:

$$\|n\| \geq n_0^{(m+1)\alpha} - (n_0^{m+1} - n)^\alpha \geq n_0^{(m+1)\alpha} - (n_0^{m+1} - n_0^m)^\alpha,$$

ja que $n \geq n_0^m$. Per acabar traiem factor comú:

$$\|n\| \geq n_0^{(m+1)\alpha} \cdot [1 - (1 - \frac{1}{n_0})^\alpha] \geq D \cdot n^\alpha.$$

Anàlogament a la inequació anterior al elevar a N arbitràriament gran tenim $\|n\| \geq n^\alpha$.

Per tant, ara tenim que $n^\alpha \leq \|n\| \leq n^\alpha$, així doncs $\|n\| = n^\alpha$ per tots els naturals. Per als enters $\|n\| = (|n|)^\alpha$, i per extensió per tot $x \in \mathbb{R}, \|x\| = |x|^\alpha$. Per tant, és una norma equivalent al valor absolut.

L'altre cas és que $\|n\| \leq 1$ per tots els naturals, per tant, si a més assumim que $\|\cdot\|$ és no trivial tindrem alguna n tal que $\|n\| < 1$.
Escollim n_0 com el natural més petit en complir això. Sabem que n_0 és primer, ja que sinó tindria divisors més petits que n_0 amb norma 1 al ser menors que n_0. Per tant el seu producte (que ésn_0) també tindria norma 1. Contradicció.

A partir d'ara anomenem p a n_0. Ara volem veure que si q és un primer diferent de p, llavors $\|q\| = 1$:
Si $\|q\| < 1$, llavors existeix un M prou gran tal que $\|p^M\|, \|q^M\|$ siguin menors que $\frac{1}{2}$. A més, al ser coprimers, podem trobar enters m i n tal que $mp^M + nq^M = 1$. I amb això trobem que

$$1 = \|1\| = \|mp^M + nq^M\| \leq \|m\|\|p^M\| + \|n\|\|q^M\| \leq \|p^M\| + \|q^M\| < \frac{1}{2} + \frac{1}{2} = 1.$$

Aquesta contradicció ens demostra que tots els primers q diferents de p tenen norma 1. Ja quasi ho tenim doncs, ja que si descomponem un enter $a = p_1^1 \cdot p_2^2 \cdot \ldots \cdot p_r^r$, i anomenem $\rho = \|p\|$, la norma de a és $\|a\| = \rho^{ord_p(a)}$, que és equivalent a la norma $\|\cdot\|_p$. □

3.2 Successions

Definició 3.15. *Diem que una successió $\{a_i\}$ de nombres racionals és de Cauchy per una norma $\|\cdot\|_p$ quan per qualsevol $\epsilon \in \mathbb{R} > 0$ tenim que existeix un enter N tal que per tot $n, m > N$, $\|a_n - a_m\|_p < \epsilon$. Dos successions $\{a_i\}, \{b_i\}$ són equivalents si $\|a_i - b_i\|_p \to 0$ quan $i \to \infty$.*

Definició 3.16. *Definim el conjunt $\mathbb{Q}_p$ com el conjunt de classes d'equivalència de successions de Cauchy amb la norma $\|\cdot\|_p$. Definim la norma d'una classe d'equivalència a com $\lim_{i\to\infty} \|a_i\|_p$*

Aquest límit està ben definit ja que:

Si $a = 0$, per definició és equivalent a la seqüència $\{0, 0, \ldots\}$ i per tant $\lim_{i\to\infty} \|a_i - 0\|_p = 0$ i ja ho hauríem enllestit.
Si $a \neq 0$, llavors existeix un enter N prou gran tal que per tot $i_N > N$ tenim que $\|a_{i_N}\|_p > \epsilon$. Si triem N prou gran tal que $\|a_i - a_{i'}\|_p < \epsilon$ per tot $i, i' > N$ llavors, pel principi de triangles isòsceles, $\|a_{i'}\|_p = max\{\|a_i\|_p, \|a_{i'} - a_i\|_p\}$. Com que hem vist que la primera (major que ϵ) és més gran que la segona (menor que ϵ) llavors, $\|a_i\|_p = \|a_{i'}\|$ per tot $i, i' > N$. Aquest és el valor comú en tots els elements d'índex major que N el que marca el valor del límit.

Tenim doncs ja una definició de $\mathbb{Q}_p$, semblant de fet a la dels reals. Seqüències infinites d'elements racionals. Definim la suma i el producte element a element. Podríem comprovar que no depèn del representant. Només hem de vigilar en el moment de fer inverses, ja que podríem tenir un 0 en una posició i dins d'una seqüència. En aquest cas, es proposa canviar el 0 per p^i i així tenim la inversa ben definida.

Per últim, per construcció gairebé, $\mathbb{Q}_p$ és complet, ja que per tota successió $\{a_j\}$ d'elements de $\mathbb{Q}_p$, és a dir, de classes d'equivalència, el seu límit és un element de $\mathbb{Q}_p$ també. Veiem'ho.
Per cada classe d'equivalència $a_j \in \mathbb{Q}_p$ tenim una successió $\{a_{ij}\}$ d'elements racionals tal que per tot parell n, m d'enters superiors a N_j, $\|a_{mj} - a_{nj}\|_p < p^{-j}$. Així doncs, la successió $\{a_{N_j j}\}$ pertany a $\mathbb{Q}_p$ i té el mateix límit que la successió $\{a_j\}$ d'elements de $\mathbb{Q}_p$.

Seguim coneixent $\mathbb{Q}_p$; el següent teorema ens dona una bona idea de com són els seus elements.

Teorema 3.17. *Tota classe d'equivalència $a \in \mathbb{Q}_p$ amb norma $\|a\|_p \leq 1$ té una única seqüència Cauchy $\{a_i\}$ representant que compleixi:*

1. $0 \leq a_i < p^i$, $a_i \in \mathbb{Z}$,
2. $a_i \equiv a_{i+1} \pmod{p^i}$.

Demostració. Mirem primer la unicitat: Si suposem que hi ha dos seqüències correctes diferents $\{a_i\}$, $\{a'_i\}$, llavors per algun i_0 hem de tenir que $a_{i_0} \not\equiv a'_{i_0} \pmod{p^{i_0}}$. Al ser tots els elements congruents entre ells aquesta diferència es manté i $\|a_i - a'_i\|_p > 1/p^{i_0}$ per a tot $i > i_0$. Contradicció.

Veiem ara l'existència, a partir d'una seqüència $\{b_i\}$ construirem una equivalent $\{a_i\}$ que compleixi les condicions. Per això necessitem el següent lema.

Lema 3.18. *Si $x \in \mathbb{Q}$ i $\|x\|_p \leq 1$, llavors per qualsevol i existeix un enter $\alpha \in \mathbb{Z}$ tal que $\|\alpha - x\|_p \leq p^{-i}$, on $\alpha \in \{0, 1, 2, \ldots, p^i - 1\}$.*

Demostració. Escrivim $x = \frac{a}{b}$ en la fracció més simplificada. Com que $\|x\|_p \leq 1$, en conseqüència p no divideix b, i, per tant, b i p^i són coprimers. Així doncs, podem trobar enters m, n tal que $mb + np^i = 1$. Assignem $\alpha = am$. La idea és que mb difereix de 1 en una quantitat p-àdicament petita. Per tant m és una bona aproximació de $1/b$ i en conseqüència am és una bona aproximació de $\frac{a}{b}$. Veiem-ho:

$$\|\alpha - x\|_p = \|am - (a/b)\|_p = \|a/b\|_p \|mb - 1\|_p \leq \|mb - 1\|_p = \|np^i\|_p = \|n\|_p / p^i \leq 1/p^i.$$

Finalment, escollim el representant de α que compleixi la segona condició i ja ho tenim. Lema demostrat. □

Retornant a la prova del teorema, si de la nostra seqüència $\{b_i\}$ escollim per $N(j)$ l'enter tal que per tot $i, i' \geq N(j)$, $\|b_i - b'_i\|_p \leq p^{-j}$.

Ara observem la seqüencia $\{b_{N_j}\}$. Veiem que $\|b_i\|_p \leq 1$ si $i \geq N(1)$, ja que per a tot $i' \geq N(1)$ es compleix:

$$\|b_i\|_p \leq \max(\|b'_i\|_p, \|b_i - b'_i\|_p) \leq \max(\|b'_i\|_p, 1/p), \|b'_i\|_p \|a\|_p \leq 1,$$

quan $i'\infty$.
Per tant, podem aplicar ara el lema a $\{b_{N(j)}\}$ i trobar una seqüència $\{a_j\}$ tal que $\|a_j - b_{N(j)}\|_p \leq 1/p^j$.
Aquesta és la seqüència que buscàvem, només falta demostrar que $a_i \equiv a_{i+1} \pmod{p^i}$ i que $\{b_j\}$ i $\{a_j\}$ tenen el mateix límit.
La primera es veu d'aquesta manera:

$$\begin{aligned}\|a_{j+1} - a_j\|_p &= \|a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})\|_p \\ &\leq \max(\|a_{j+1} - b_{N(j+1)}\|_p, \|b_{N(j+1)} - b_{N(j)}\|_p, \|a_j - b_{N(j)}\|_p) \\ &\leq \max(1/p^{j+1}, 1/p^j, 1/p^j) = 1/p^j.\end{aligned}$$

Aquesta diferència implica que $a_{j+1} \equiv a_j \pmod{p^j}$. Veiem ara que tenen el mateix límit. Veiem que per $i > N(j)$

$$\begin{aligned}\|a_i - b_i\|_p &= \|a_i - a_j + a_j - b_{n(j)} - (b_i - b_{N(j)})\|_p \\ &\leq \max(\|a_i - a_j\|_p, \|a_j - b_{n(j)}\|_p, \|b_i - b_{N(j)}\|_p) \\ &\leq \max(1/p^j, 1/p^j, 1/p^j) = 1/p^j.\end{aligned}$$

Per tant, tenen el mateix límit. El teorema està demostrat. □

Bàsicament el que acabem de demostrar es que la notació $(a_0, a_1, a_2, \ldots)$ que fèiem servir és adequada per tots els elements de $\mathbb{Q}_p$ amb norma menor que 1.
Tot i això, què passa amb els elements amb norma major que 1? Si $\|a\|_p = p^m$ hem de multiplicar a per p^m per obtenir $a' = ap^m$ que té norma menor que 1 per tant té representació com hem determinat abans. Llavors escrivim a' en expansió p-àdica:

$$a' = b_0 + b_1 p + b_2 p^2 + \ldots + b_i p^i + \ldots.$$

Per tant, com que $a' = ap^{-m}$, podem imaginar-nos l'element a com:

$$a' \cdot p^{-m} = a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \frac{b_2}{p^{m-2}} + \ldots + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + \ldots.$$

Semblant a un nombre decimal limitat.

I és aquí quan topem amb una altra definició per $\mathbb{Z}_p$. Aquesta més treballada.

Definició 3.19. *Anomenem $\mathbb{Z}_p$ al conjunt d'elements de $\mathbb{Q}_p$ amb norma menor o igual que 1. $\mathbb{Z}_p = \{a \in \mathbb{Q}_p | \|a\|_p \leq 1\}$.*

Per les propietats de la norma p-àdica és fàcil saber que la suma i la multiplicació en $\mathbb{Z}_p$ són tancades. Per tant, $\mathbb{Z}_p$ és un subanell de $\mathbb{Q}_p$.
Ara indaguem una mica en $\mathbb{Q}_p$. Primer de tot escrivim $a \equiv b \pmod{p^n}$ si $\|a-b\|_p \leq p^{-n}$, o el que és el mateix, que els primers coeficients de l'expansió p-àdica de $a - b$ fins el coeficient que acompanya p^n siguin 0. També, com ja vam veure al capítol dels nombres p-àdics, un element de $\mathbb{Z}_p$ és invertible si i només si no es pot dividir per p. Per tant,

aquests elements tenen norma 1: ja que si x i $1/x \in \mathbb{Z}_p$, llavors $\|x\|_p \geq 1$ i $\|x\|_p \leq 1$. Quan $\|x\|_p = 1$, diem que x és una unitat p-àdica.

Veiem ara que una expansió p-àdica està ben definida, ja que la suma infinita és convergent en $\mathbb{Q}_p$ si i només si el terme general tendeix a 0, per la propietat de la norma no-arquimediana. No tenim cap cas com en els racionals en el que $\sum_{i=0}^{n} 1/i$ tendeix a infinit encara que el terme general tendeixi a 0.

Observació 3.20. L'expansió p-àdica, incluint els elements amb norma negativa, és única per cada element de $\mathbb{Q}_p$. En canvi, en els racionals expressats en base 10 no és així, ja que $1 = 0,9999\ldots$

Per acabar aquest tema, una curiositat: en comptes de $\{0, 1, 2, \ldots, p-1\}$ podríem haver triat qualsevol conjunt $\{\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{p-1}\}$ on $\alpha_i \equiv i \pmod{p}$ i haver definit l'expansió p-àdica com $\sum_{i=-m}^{\infty} b_i p^i$. En general no és de gran utilitat excepte en alguns casos, on ens poden ser útil els ja esmentats "Teichmüller representatives".

3.3 Lema de Hensel

En aquest capítol veurem com funcionen les arrels a $\mathbb{Q}_p$ i veurem quan els polinomis tenen zeros en $\mathbb{Q}_p$ i quan no. Encara no ens hem fet una idea completa de la magnitud de $\mathbb{Q}_p$. Potser xoca saber que, per exemple, $\sqrt{2}$ ó $\sqrt{23}$ pertanyen a $\mathbb{Q}_7$.

Calculem doncs, $\sqrt{23}$:

Imposem $(a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + a_3 \cdot 7^3 + \ldots)^2 = 2 + 3 \cdot 7$. Si calculem el producte veiem que $a_0^2 + 2a_1a_0 \cdot 7 + (a_1^2 + 2a_0a_2) \cdot 7^2 + (2a_0a_3 + 2a_1a_2) \cdot 7^3 + \ldots = 2 + 3 \cdot 7$. En aquest moment si mirem congruències modul 7 tenim que $a_0^2 = 2$, per tant, a_0 ha de ser 3 o 4. Ens quedem amb el 3.
Ara mirem congruències modul 7^2. Tenim que $9 + 6a_1 \cdot 7 \equiv 2 + 3 \cdot 7 \pmod{7^2}$ si i només si $6a_1 \cdot 7 \equiv 2 - 9 + 3 \cdot 7 \equiv 2 \cdot 7 \pmod{7^2}$, que és equivalent a $6a_1 \equiv 2 \pmod{7}$ que sempre té solució al ser $\mathbb{Z}/7\mathbb{Z}$ domini d'integritat. En aquest cas, $a_1 = 5$. Repetim el pas fet fins ara, $9 + 30 \cdot 7 + (25 + 6a_2) \cdot 7^2 \equiv 2 + 3 \cdot 7 \pmod{7^3} \Leftrightarrow 28 \cdot 7 + (25 + 6a_2) \cdot 7^2 \equiv 0 \pmod{7^3} \Leftrightarrow (29 + 6a_2) \cdot 7^2 \equiv (1 + 6a_2) \cdot 7^2 \equiv 0 \pmod{7^3}$. I, com abans, això succeeix si i només si $6a_2 \equiv -1 \pmod{7}$. Per tant, $a_2 = 1$. Repetiríem el procés amb congruències modul 7^4 i arribaríem a la conclusió que $6a_3 \equiv 6 \pmod{7}$ i per tant, tindríem $a_3 = 1$. Així successivament podríem aproximar infinitament l'arrel de 23 en $\mathbb{Q}_p$. De moment sabem que $\sqrt{23} = 3 + 5 \cdot 7 + 1 \cdot 7^2 + 1 \cdot 7^3 + \ldots$.

Si haguéssim assignat 4 en comptes de 3 a a_0 haguéssim trobat una altra arrel, que de fet es correspon amb el negatiu de l'arrel que hem trobat.

Aquesta innocent arrel que hem trobat ens obre molts dubtes. Tots els elements de $\mathbb{Q}_7$ tenen arrel? I els de $\mathbb{Q}_p$? És numerable $\mathbb{Q}_p$? i $\mathbb{Z}_p$? Quins polinomis tenen solució en $\mathbb{Q}_p$? Poc a poc intentarem resoldre tots els dubtes.

Per començar, veiem que si 3 tingués arrel $a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \ldots$ a $\mathbb{Q}_7$, llavors s'hauria de complir que $a_0 \equiv 3 \pmod{7}$ i això és impossible ja que 3 no és un quadrat en $\mathbb{Z}/7\mathbb{Z}$. Per tant, com més aviat demostrarem, les unitats de $\mathbb{Q}_p$, per p diferent de 2,

només tenen arrel si el seu representant en modul p és un quadrat. Quan no són unitats llavors es una mica més complicat. Tot element x de $\mathbb{Q}_p$ es pot expressar com $x = p^n u$, on u és una unitat. De fet p^n coincideix amb la norma p-àdica de x. Si n és parell x té arrel si i només si u té arrel. Aquesta seria $\sqrt{x} = p^{n/2} \cdot \sqrt{u}$. Si n és imparell no té arrel, ja que això significaria

$$\|x\|_p = (\|\sqrt{x}\|_p)^2 = (p^\lambda)^2 = p^{2\lambda} = p^n \Leftrightarrow 2\lambda = n.$$

Contradicció, ja que la norma dels elements de $\mathbb{Q}_p$ només pren valor en les potències de p.

En quant a la numerabilitat de $\mathbb{Z}_p$ podem veure que l'argument de la diagonal de cantor ens demostra que $\mathbb{Z}_p$ és no numerable. Si hi hagués una successió infinita amb tots els elements de $\mathbb{Z}_p$ escrits en expansió p-àdica podríem construir un nou element on el coeficient i-éssim és coeficient i-éssim de l'element i-éssim de la successió més 1. Per tant, hauríem construït un element de $\mathbb{Z}_p$ diferent en almenys un coeficient (diferent en qualsevol cas) a tots els elements de la successió. Contradicció.

$\mathbb{Z}_p$ és doncs no-numerable i $\mathbb{Q}_p$ en conseqüència tampoc.

Tot això ens porta inevitablement al lema de Hensel, en el qual veurem que trobar solucions a polinomis en $\mathbb{Q}_p$ és relativament senzill i el procediment és bastant similar al que hem fet servir per trobar l'arrel de 23.

Teorema 3.21. *(Lema de Hensel). Sigui $F(x) = c_0 + c_1 x + \ldots + c_n x^n$ un polinomi amb enters p-àdics com a coeficients. I sigui $F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \ldots + n c_n x^{n-1}$ la derivada de $F(x)$. Si tenim un enter p-àdic a_0 tal que $F(a_0) \equiv 0 \pmod p$ i tal que $F'(a_0) \not\equiv 0 \pmod p$, llavors existeix un únic enter p-àdic a tal que $F(a) = 0$ i $a \equiv a_0 \pmod p$.*

(Nota: en el cas anterior teníem $F(x) = x^2 - 23$, $F'(x) = 2x$, $a_0 = 3$.)

Demostració. Volem demostrar que existeix una seqüència única d'enters racionals $a_1, a_2, \ldots$ tal que per tot $n \geq 1$:
$F(a_n) \equiv 0 \pmod{p^{n+1}}$,
$a_n \equiv a_{n-1} \pmod{p^n}$,
$0 \leq a_n \leq p^{n+1}$.

Ho demostrarem per inducció.

Per n=1, a_1, complint les dues últimes condicions, ha de ser de la forma $a_1 = a_0 + b_1 p$, on $b_1 \in \mathbb{Z}/p\mathbb{Z}$. Ara només queda veure la primera, $F(a_1) \equiv 0 \pmod{p^2}$. Això serà si:

$$\begin{aligned} F(a_0 + b_1 p) &= \sum c_i (a_0 + b_1 p)^i = \sum (c_i a_0^i + i c_i a_0^{i-1} b_1 p + \text{termes divisibles per } p^2). \\ &\equiv \sum c_i a_0^i + (\sum i c_i a_0^{i-1}) b_1 p \pmod{p^2} = F(a_0) + F'(a_0) b_1 p \end{aligned}$$

(Notem la similitud amb el Taylor que coneixem. $F(x+h) = F(x) + F'(x)h$+termes d'orde superior). Com que $F(a_0) \equiv 0 \pmod p$, podem assumir $F(a_0) \equiv \alpha p \pmod{p^2}$, per algun $\alpha \in \mathbb{Z}/p\mathbb{Z}$. Així que si imposem que $F(a_1) \equiv 0 \pmod{p^2}$ obtenim:

$$\begin{aligned} &\alpha p + F'(a_0) b_1 p \equiv 0 \pmod{p^2} \\ \Leftrightarrow\ &\alpha + F'(a_0) b_1 \equiv 0 \pmod p. \end{aligned}$$

Per tant b_1 queda perfectament i adequadament determinat per $b_1 = -\frac{\alpha}{F'(a_0)}$ ja que $F'(a_0)$ és diferent de 0.
Cas inicial demostrat, ara anem al cas general.

Suposem que ja tenim $a_0, a_1, a_2, \ldots, a_{n-1}$ que compleixen les condicions. Volem trobar doncs a_n. Sabem que $a_n = a_{n-1} + b_n p^n$. A partir d'aquí la demostració és bastant anàloga al cas inicial. Tenim:

$$F(a_n) = F(a_{n-1} + b_n p^n) \equiv F(a_{n-1}) + F'(a_{n-1}) b_n p^n \pmod{p^{n+1}}.$$

Afegim que $F(a_{n-1}) \equiv \alpha p^n \pmod{p^{n+1}}$ ja que $F(a_{n-1}) \equiv 0 \pmod{p^n}$. Per tant podem reduir la congruència a una congruència mòdul p. Ja que $F(a_{n-1}) + F'(a_{n-1}) b_n p^n \equiv \alpha p^n + F'(a_{n-1}) b_n p^n \pmod{p^{n+1}}$ és equivalent a $\alpha + F'(a_{n-1}) b_n \equiv 0 \pmod{p}$. Si tenim en compte també que per hipòtesis $a_{n-1} \equiv a_0$, llavors $F'(a_{n-1}) \equiv F'(a_0) \not\equiv 0$. Llavors tenim b_n perfectament i adequadament determinat com $\frac{\alpha}{F'(a_0)} \pmod{p}$.

Un cop complerta la inducció ja tenim el teorema demostrat, ja que si assignem $a = a_0 + b_1 p - b_2 p^2 + \ldots$ tenim $F(a) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}}$ per tot enter positiu n. Per tant $F(a) = 0$ i $a \equiv a_0 \pmod{p}$. Alternativament, el fet d'existir una altra solució implicaria la existència d'una altra seqüència $a = a_0 + b_1 p + b_2 p^2 + \ldots$ però aquesta és única com hem vist. □

És notable la similitud entre el lema de Hensel i el mètode de Newton per aproximar arrels. Per trobar el següent iterat amb el mètode Newton usem la formula $a_n - a_{n-1} = -\frac{f(a_{n-1})}{f'(a_{n-1})}$ i Hensel per trobar el nou coeficient usa $b_n p^n \equiv -\frac{\alpha p^n}{F'(a_{n-1})} \pmod{p^{n+1}}$. Però la diferència és que el mètode Newton en els reals s'usa per aproximar solucions però no s'usa per demostrar la seva existència com en el lema de Hensel ja que Newton no sempre convergeix en els reals com ja sabem. En canvi, en els nombres p-àdics i per les condicions donades sí. Es pot generalitzar el lema de Hensel:

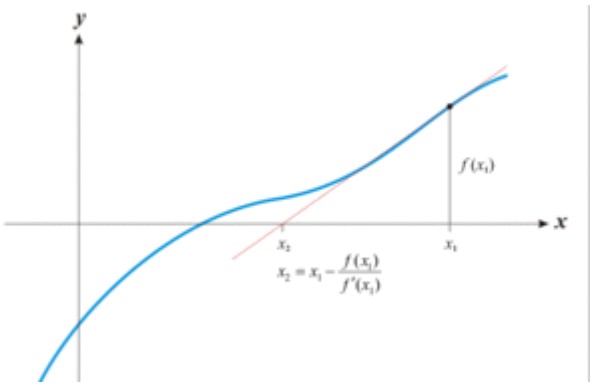


Figura 2: Producte

Proposició 3.22. *Sigui $F(x)$ un polinomi amb enters p-àdics com a coeficients. Si a_0 compleix $F'(a_0) \equiv 0 \pmod{p^M}$ però $F'(a_0) \not\equiv 0 \pmod{p^{M+1}}$, i a més $F(a_0) \equiv 0 \pmod{p^{2M+1}}$, llavors existeix una única $a \in \mathbb{Z}_p$ tal que $F(a) = 0$ i $a \equiv a_0 \pmod{p^{M+1}}$.*

Demostració. La demostració és bastant anàloga al lema de Hensel. Fem una inducció on el cas general és M. Volem anar construint una successió $a_0 + b_{M+1} p^{M+1} + b_{M+2} p^{M+2} + \ldots$

tal que cada successió parcial M-èssima compleixi que $F(a_M + i) \equiv 0 \pmod{p^{2M+i+1}}$

Per les característiques que hem definit sabem que $F'(a_0) \equiv \alpha p^M \pmod{p^{M+1}}$, on $\alpha \in \mathbb{Z}/p\mathbb{Z}$. També sabem que:

$$F(a_0 + b_{M+1}p^{M+1}) \equiv F(a_0) + F'(a_0)b_{M+1}p^{M+1} \equiv \beta p^{2M+1} + \alpha p^M \cdot p^{M+1} \pmod{p^{2M+2}}.$$

Imposem que sigui 0 i tenim que b_{M+1} queda únicament determinada.

I per el cas general similar:

$$\begin{aligned} F(a_{M+n} + b_{M+n}p^{M+n}) &\equiv F(a_{M+n}) + F'(a_{M+n})b_{M+n}p^{M+n} \\ &\equiv \alpha' p^{2M+n} + \beta' b_{M+n}p^M \cdot p^{M+n} \pmod{p^{2M+n+1}}. \end{aligned}$$

Que és equivalent a $\alpha' + \beta' b_{M+n} \equiv 0 \pmod{p}$.
Per tant, b_{M+n} queda únicament determinada i

$$a_{M+n} = a_0 + b_{M+1}p^{M+1} + b_{M+2}p^{M+2} + \ldots + a_{M+n}p^{M+n},$$

compleix les hipòtesis de inducció.

Per últim, el límit de la seqüència a_{M+n} és la solució. □

3.4 Quadrats a $\mathbb{Q}_p$

Per a $p \neq 2$ ja hem vist que per a $x \in \mathbb{Z}_p$, x és arrel si i només si x és quadrat a $(\mathbb{Z}/p\mathbb{Z})^*$. També sabem que tot element x de $\mathbb{Q}_p$ es pot representar de manera única com $x = p^n \cdot u$, on $n \in \mathbb{Z}$ i $u \in \mathbb{Z}_p$ i també hem demostrat que si la potència de p és imparell llavors x no pot ser un quadrat. Tot això fa que $[\mathbb{Q}_p^* : (\mathbb{Q}_p^2)^*] = 2 \cdot 2 = 4$.

No és tant clar que passa quan $p = 2$. Per sort tenim una proposició:

Proposició 3.23. *Una unitat $u \in \mathbb{Z}_2^*$ és un quadrat si i només si $u \equiv 1 \pmod{8}$.*

Demostració. Apliquem el lema de Hensel generalitzat amb $f(x) = x^2 - u$ i $a_0 = 1$. Tenim que $F(a_0) \equiv 0 \pmod{8}$ i $F'(a_0) = 2 \not\equiv 0 \pmod{4}$. Així doncs tindríem una solució a tal que $F(a) = 0$ i $a \equiv 1 \pmod{8}$. També és fàcil comprovar que a $\mathbb{Z}/8\mathbb{Z}$ no hi ha cap més quadrat que no sigui parell. Per tant la seva derivada en mòdul 4 seria congruent amb 0 i no podríem aplicar Hensel. □

Quedem doncs que $[\mathbb{Q}_2^* : (\mathbb{Q}_2^2)*] = 8$.

4 Formes quadràtiques i espais quadràtics

El teorema de Hasse-Minkowski, la meta d'aquest treball, ens relaciona els nombres racionals amb els nombres p-àdics mitjançant les formes quadràtiques. Així que en aquest capítol veurem i demostrarem tot el que necessitem saber sobre formes quadràtiques per entendre el teorema de Hasse-Minkowski i la seva demostració.

Definició 4.1. *Sigui K un cos i E un espai vectorial, una forma bilineal és una aplicació $f : E \times E \to K$ que compleix:*

1. $f(u_1 + u_2, v) = f(u_1, v) + f(u_2, v)$,
2. $f(u, v_1 + v_2) = f(u, v_1) + f(u, v_2)$,
3. $f(au, v) = a \cdot f(u, v) = f(u, av)$.

Per a tot $a \in K$, i per a tot $u, v, u_1, u_2, v_1, v_2 \in E$.

Una definició equivalent és veure les formes bilineals com un producte de vectors i matrius.

Definició 4.2. *Una forma bilineal és una aplicació $F : E \times E \to K$ definida per $F(U, V) = U^t \cdot M \cdot V$, on U, V són vectors pertanyents a E i M és una matriu, de la mateixa dimensió que els vectors.*

És fàcil veure que aquesta notació compleix les propietats de la notació anterior.

Exemple 4.3. El producte escalar de dos vectors $A = (x_1, y_1, z_1)$ i $B = (x_2, y_2, z_2)$ és una forma bilineal que es defineix per $f(A, B) = x_1x_2 + y_1y_2 + z_1z_2$ és el resultat de multiplicar $A^t \cdot M \cdot B$, on $M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Seguint amb la forma matricial és fàcil veure que, per dimensió 3 per exemple, totes les formes bilineals són de l'estil

$$ax_1y_1 + bx_1y_2 + cx_1y_3 + dx_2y_1 + ex_2y_2 + fx_2y_3 + gx_3y_1 + hx_3y_2 + ix_3y_3.$$

Definició 4.4. *Una forma bilineal és simètrica quan la seva matriu representativa M és simètrica.*

Una forma bilineal simètrica compleix que $f(a, b) = f(b, a)$.

Definició 4.5. *Una forma quadràtica és un polinomi en el que tots els monomis tenen exactament grau 2.*

Definim la forma quadràtica ϕ a través de la forma bilineal simètrica ψ, en tant que $\phi(u) = \psi(u, u)$ i veiem que òbviament la forma serà de l'estil $\sum a_{i,i}x_i^2 + \sum_{i<j} a_{i,j}x_ix_j$ per tant és obvi que tots els monomis tenen grau 2.

Veiem que alhora ϕ defineix ψ ja que $\psi(u, v) = (\phi(u + v) - \phi(u - v))/4$. Veiem-ho:

$$\begin{aligned} \phi(u + v) &= \psi(u + v, u + v) = \psi(u, u) + 2\psi(u, v) + \psi(v, v), \\ \phi(u - v) &= \psi(u - v, u - v) = \psi(u, u) - 2\psi(u, v) + \psi(v, v). \end{aligned}$$

Així que tenim diferents igualtats:

$$\begin{aligned} 2 \cdot \psi(u, v) &= \phi(u + v) - \phi(u) - \phi(v), \\ 2 \cdot \psi(u, v) &= \phi(u) + \phi(v) - \phi(u + v), \\ 4 \cdot \psi(u, v) &= \phi(u + v) - \phi(u - v). \end{aligned}$$

Per tant, d'ara en endavant suposarem que k té caràcter diferent de 2.

Veiem doncs que ψ és no-nul·la si i només si ϕ tampoc ho és. Al ser $\psi(u,v) \neq 0$ per algun parell $(u,v) \in E^2$, llavors entre $\phi(u+v)$ i $\phi(u-v)$ algun ha de ser diferent de 0.

Definició 4.6. *Un espai quadràtic és un parell (E,ψ) que consisteix en un k-espai vectorial E i una forma bilineal simètrica $\psi : E \times E \to K$.*

Definició 4.7. *Un espai quadràtic és regular quan ψ és no-degenerada, és a dir, la funció lineal $\omega_v(u) = \psi(u,v)$ és no-nul·la per qualsevol $v \in E$ diferent de 0.*

Exemple 4.8. La forma bilineal $\psi((x_1,y_1),(x_2,y_2)) = (x_1+y_1)\cdot(x_2+y_2)$ és no-regular ja que si $(x_1,y_1) = (1,-1)$ el resultat serà sempre 0.

Proposició 4.9. *El parell (U,ψ) és regular si i només si per qualsevol base $(u_1,\ldots,u_n)$ de E tenim que* $\det[\psi(u_i,u_j)] \neq 0$.

Del contrari, si $\det[\psi(u_i,u_j)] = 0$, existiria algun vector V, tal que $M \cdot V$ és 0, per tant, $\omega_V(u) = \psi(u,v)$ seria nul·la, i en conseqüència, ψ seria degenerada i el parell (E,ψ) no-regular.

Aquest nombre, $\delta(\phi) = \delta(\psi) = \det[\psi(u_i,u_j)]$ és important, l'anomenem determinant. No està ben definit, ja que no hi ha base canònica de E. Per tant, el considerem mòdul quadrat, com un element de $K^*/(K*)^2$.

Definició 4.10. *Per un subespai V de l'espai quadràtic (E,ψ), tal que $V \subseteq E$, definim el seu complement ortogonal (respecte a ψ) com:*

$$V^\perp = \{u \in E \mid \psi(u,v) = 0, \text{ per a tot } v \in V\}$$

Proposició 4.11. *Si (E,ψ) és regular llavors* $\dim V + \dim V^\perp = \dim E$.

Demostració. Considerem la base $(v_1,v_2,\ldots,v_m)$ del subespai V i definim la funció:

$$\begin{aligned} U &\to V \\ u &\mapsto (\psi(u,v_1),\psi(u,v_2),\ldots,\psi(u,v_m)). \end{aligned}$$

La imatge està definida en la base $v_1,..,v_m$ que hem definit abans. Com que ψ és regular, aquesta funció és exhaustiva. I el nucli n'és $V^\perp$. Demostrat. □

Podríem pensar que un subespai i el seu component ortogonal són complementaris però no sempre succeeix, ja que podem tenir $V^\perp \cap V \neq \{0\}$. El que sempre és cert és el següent:

Proposició 4.12. *Sigui E un espai regular i V el seu subespai, llavors $(V^\perp)^\perp = V$.*

Demostració. Els elements de $(V^\perp)^\perp$ són els ortogonals amb tots els element de $V^\perp$ i els elements de V compleixen aquesta condició, per tant, $V \subseteq (V^\perp)^\perp$.
Per altra banda,

$$\begin{aligned} \dim V + \dim V^\perp &= \dim U \\ \dim(V^\perp)^\perp + \dim V^\perp &= \dim U. \end{aligned}$$

Aquest sistema d'equacions que ens porta a veure que $\dim V = \dim(V^\perp)^\perp$, i per tant $V = (V^\perp)^\perp$. □

Proposició 4.13. *Sigui V un subespai regular de (E, ψ). Llavors $E = V \oplus V^{\perp}$.*

Observació 4.14. Previ a la demostració és important veure que el conjunt que és regular és V, de fet E no té perquè ser-ne.

Demostració. Veiem que $V \cap V^{\perp} = \{0\}$, ja que, del contrari, existiria $u \in V$ tal que $\psi(u, v) = 0$ per a tot $v \in V$. Això significaria que V no és regular.

Només queda veure que $V + V^{\perp} = E$. Hem de veure que tot $u \in E$ és resultat de la suma d'elements de V o de $V^{\perp}$. Sigui quin sigui el valor de $\psi(u, v)$, per cada $u \in E$ tindrem $w \in V$ tal que $\psi(u, v) = \psi(w, v)$. Això provoca que $u - w \in V^{\perp}$ ja que $\psi(u - w, v) = \psi(w, v) - \psi(u, v) = 0$. Per tant podem expressar u com $u = w + (u - w)$ suma d'elements de V i el seu component ortogonal, per tant $E = V \oplus V^{\perp}$. □

Observació 4.15. Quan un subespai V és regular no té intersecció amb el seu component ortogonal i a l'inrevés. De la mateixa manera, $V \cap V^{\perp} = \{0\}$ si i només si $V^{\perp}$ regular. Tenim una triple equivalència.

Definició 4.16. *Una base $(u_1, u_2, \ldots, u_m)$ de E és ortogonal si $\psi(u_i, u_j) = 0$ per a tot $i \neq j$.*

Proposició 4.17. *Qualsevol espai quadràtic E admet una base ortogonal.*

Demostració. Si ϕ és nul·la qualsevol base serveix. Si no ho és, tenim algun element u_1 tal que $\phi(u_1) \neq 0$. Considerem doncs el component ortogonal de $V =< u_1 >$, el conjunt $V^{\perp}$ i repetim el procés ara per trobar u_2 dins de $V^{\perp}$. Ara el nou conjunt serà el component ortogonal de $< u_1, u_2 >$. El procés és finit i genera una base ortogonal $(u_1, u_2, \ldots, u_m)$. □

Observació 4.18. Si E és regular els elements de la base ortogonal compleixen $\phi(u_i) \neq 0$.

4.1 Isotropia

Estudiem com es comporten les solucions de formes quadràtiques.

Definició 4.19. *Un element $u \neq 0$ que compleix $\phi(u) = \psi(u, u) = 0$ es diu isotròpic (respecte a ψ). També diem que un espai quadràtic (E, ψ) és isotròpic si té com a mínim un element isotròpic.*

Exemple 4.20. La forma quadràtica ψ amb matriu $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ quan té base $\{u, v\}$ i que per a un element $(xu + yv)$, resulta $\phi(xu + yv) = 2xy$.

D'aquest espai quadràtic en diem **pla hiperbòlic**.

Definició 4.21. *D'una forma quadràtica de dos variables $q(x_1, x_2)$ en diem que és un pla hiperbòlic si:*

$$q(x_1, x_2) \sim x_1 x_2 \sim x_1^2 - x_2^2.$$

Seguim parlant d'isotropia.

Exemple 4.22. Qualsevol parell (E, ψ) no regular és isotròpic.

Com hem vist en l'exemple anterior la inversa no és certa.

Proposició 4.23. *Sigui (E, ϕ) un espai quadràtic isotròpic regular, llavors $E = V \times V^{\perp}$, on V és el pla hiperbòlic.*

L'important d'aquesta proposició està en veure que pel sol fet de ser isotròpic, immediatament es té un pla hiperbòlic, després la suma de subespais és lògica al ser E regular.

Demostració. Al ser (ψ) isotròpica, tenim un element $u \in E$ que compleix $\psi(u, u) = 0$. Al ser (E, ϕ) regular, tenim un element diferent que compleix $\psi(w, w) \neq 0$, podem assumir que $\psi(w, w) = 1$. Ara considerem el vector $v = \lambda u + w$, on $\lambda \in K$.

$$\psi(u, v) = \psi(u, \lambda u + w) = \lambda\psi(u, u) + \psi(u, w) = 1$$
$$\psi(v, v) = \lambda^2\psi(u, u) + 2\lambda\psi(u, w) + \psi(w, w) = 2\lambda + \psi(w, w)$$

Escollim $\lambda = -\frac{1}{2}\psi(w, w)$ i tenim que $\psi(v, v) = 0$. Per tant, en el subespai $V =< u, v >$ tenim el pla hiperbòlic. □

Definició 4.24. *Un espai quadràtic (E, ψ) és universal quan per a tot $\alpha \in K^*$ existeix $u \in E$ tal que $\psi(u, u) = \alpha$. En aquest cas diem que ψ representa α.*

Exemple 4.25. En el cas que el cos K siguin els reals. La forma quadràtica és isotròpica si i només si és equivalent a una forma

$$x_1^2 + x_2^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_n^2,$$

en el que $0 < r < n$. En aquest cas, també és universal.

La isotropia i la universalitat estan relacionades, però fins a quin punt? Veiem-ho.

Proposició 4.26. *Qualsevol espai regular isotròpic (E, ψ) és universal.*

Demostració. Al ser isotròpica conté el pla hiperbòlic que és universal. □

El recíproc no és sempre cert, existeixen formes quadràtiques universals però no isotròpiques.

Teorema 4.27. *Essent K un cos finit amb característica diferent de 2, qualsevol espai quadràtic regular sobre K de dimensió ≥ 2 és universal.*

Demostració. Podem suposar que l'espai és de dimensió 2 i u, v en formen base ortogonal. Per tant,

$$\phi(xu + yv) = x^2\phi(u) + y^2\phi(v),$$

on $\phi(u), \phi(v) \neq 0$. Si $K = \mathbb{F}_q$, llavors K^* és un cíclic d'ordre $q - 1$, i el seu subgrup de quadrats té ordre $\frac{q-1}{2}$.

Per tant, en K tenim $\frac{q+1}{2}$ quadrats (li hem afegit el 0). Així que el conjunt de nombres que es poden expressar com $x^2\phi(u)$ té ordre $\frac{q+1}{2}$.

Ara, per un α qualsevol pertanyent a $\mathbb{F}_q$, el conjunt $\{\alpha - y^2\phi(v) | v \in \mathbb{F}_q\}$ també té ordre $\frac{q+1}{2}$, els conjunts no poden ser disjunts. No poden ser disjunts al sumar $q+1$ elements en un cos de q elements. Per tant, existeix un element $\beta \in \mathbb{F}_q$ tal que:

$$\beta = x^2\phi(u) = \alpha - y^2\phi(v)$$

Hem vist que per a tot $\alpha \in K$ existeixen x, y tal que:

$$\phi(xu + yv) = x^2\phi(u) + y^2\phi(v) = \alpha.$$

Per tant, és universal. □

En canvi, una forma quadràtica en un espai finit com podria ser

$$\phi(xu + yv) = x^2 \cdot 1 - y^2 \cdot \beta,$$

on β no és un quadrat és universal (com hem vist en el teorema anterior) però en K no és isotròpica.

Observació 4.28. Universalitat no implica isotropia.

Proposició 4.29. *La forma quadràtica $\phi(x_1, x_2, \ldots, x_n)$ representa $\alpha \in K^*$ si i només si $\phi(x_1, x_2, \ldots, x_n) - \alpha Y^2$ és isotròpic.*

Demostració. La primera implicació és trivial. En la segona hem d'observar dos casos: Si $y = 0$, llavors $\phi(x_1, \ldots, x_n)$ és isotròpica, per tant universal, per tant representa α. En el segon cas ($y \neq 0$) tenim una solució $(x_1^*, x_2^*, ..., x_n^*)$ que compleix $\phi(x_1^*, x_2^*, ..., x_n^*) - \alpha y^2 = 0$. Per tant, $\phi(\frac{x_1^*}{y}, \frac{x_2^*}{y}, ..., \frac{x_n^*}{y},) = \alpha$. □

Com a resultat de l'anterior proposició tenim la següent proposició sobre la isotropia:

Proposició 4.30. *Qualsevol forma quadràtica de 3 variables o més en un cos finit és isotròpica.*

Demostració. Si la forma no és regular, immediatament passa a ser isotròpica.
Si la forma és regular la podem expressar com

$$\phi(x_1, x_2, x_3) = \alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2$$

Podem veure $\alpha_1 x_1^2 + \alpha_2 x_2^2$ com una altra forma quadràtica que al tenir dos variables és universal, per tant representa $-\alpha_3$. Per últim, fent servir la proposició anterior això és equivalent a demostrar la isotropia de ϕ. □

Proposició 4.31. *Siguin $f(X)$ i $g(Y)$ formes quadràtiques regulars en un cos K. Si $f(X) - g(Y)$ és isotròpic llavors existeix un $\alpha \in K^*$ representat per les dues formes.*

Demostració. Al ser isotròpica la seva resta tenim que existeix un parell $(x, y) \neq 0$ d'elements de E tal que $f(x) - g(y) = 0$. Per tant, $f(x) = g(y) = \beta$. Si $\beta \neq 0$, ja hem acabat, β és el α que buscàvem. Si $\beta = 0$, f és isotròpica i per tant pot representar qualsevol valor que representi g. □

4.2 Bases ortogonals

Proposició 4.32. *(Transformació de bases). Sigui (E, ϕ) espai quadràtic amb dues bases ortogonals $\overline{\mathrm{u}} = (u_1, \ldots, u_m)$ i $\overline{\mathrm{v}} = (v_1, \ldots, v_m)$, llavors existeix una seqüència*

$$\overline{\mathrm{u}} = \overline{\mathrm{u}}_0, \overline{\mathrm{u}}_1, \ldots, \overline{\mathrm{u}}_m = \overline{\mathrm{v}},$$

on $\overline{\mathrm{u}}_i$ i $\overline{\mathrm{u}}_{i+1}$ tenen com a màxim dos vectors diferents.

Demostració. Només cal veure que podem transformar $\overline{\mathrm{u}} = (u_1, \ldots, u_m)$ a una base de la forma $(v_1, v_2^* \ldots, v_m^*)$ on només un altre (a part de u_1) dels coeficients nous u_i^* és diferent de l'original u_i.
Escrivim $v_1 = \alpha_1 u_1 + \ldots + \alpha_m u_m$. Assumim que a partir del terme s els termes $\alpha_{s+1}, \ldots, \alpha_m = 0$. Per tant, $v_1 = \alpha_1 u_1 + \ldots + \alpha_s u_s$. Tenim $\alpha \neq 0$.

Si $s = 1$, $v_1 = \alpha_1 u_1$, i per $v_2^* = u_2, \ldots, v_m^* = u_m$. Ja hem aconseguit el que volíem fent un sol canvi.

Si $s \geq 2$ i $\phi(\alpha_1 u_1 + \alpha_2 u_2) \neq 0$, considerem $u_1' = \alpha_1 u_1 + \alpha_2 u_2$. Trobem u_2' de la forma $\beta_1 u_1 + \beta_2 u_2$ tal que $\psi(u_1', u_2') = 0$:

$$\begin{aligned}\psi(u_1', u_2') &= \psi(\alpha_1 u_1 + \alpha_2 u_2, \beta_1 u_1 + \beta_2 u_2),\\ &= \alpha_1\beta_1\psi(u_1', u_1') + \alpha_1\beta_2\psi(u_1', u_2') + \alpha_2\beta_1\psi(u_2', u_1') + \alpha_2\beta_2\psi(u_2', u_2'),\\ &= \alpha_1\beta_1\phi(u_1') + \alpha_2\beta_2\phi(u_2').\end{aligned}$$

Escollim $\beta_1 = \alpha_2\phi(u_2')$ i $\beta_2 = -\alpha_1\phi(u_1')$. Tenim $(\beta_1, \beta_2) \neq 0$ ja que

$$\phi(\alpha_1 u_1 + \alpha_2 u_2) = \alpha_1^2\phi(u_1) + \alpha_2^2\phi(u_2) \neq 0$$

Si $s \geq 2$ i $\phi(\alpha_1 u_1 + \alpha_2 u_2) = 0$, llavors no és possible per $s = 2$, (ja que $v_1 = \alpha_1 u_1 + \alpha_2 u_2$ no és isotròpica). Tenim que s ha de ser ≥ 3. Per tant considerem els tres vectors següents:

$$\begin{aligned}&\alpha_1 u_1 + \alpha_2 u_2,\\ &\alpha_1 u_1 + \alpha_3 u_3,\\ &\alpha_2 u_2 + \alpha_3 u_3.\end{aligned}$$

Almenys uns dels tres no és isotròpic, ja que, de ser-ho, tindríem:

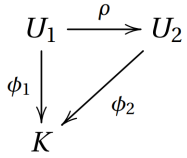
$$\begin{aligned}\alpha_1^2\phi(u_1) + \alpha_2^2\phi(u_2) &= 0,\\ \alpha_1^2\phi(u_1) + \alpha_3^2\phi(u_3) &= 0,\\ \alpha_2^2\phi(u_2) + \alpha_3^2\phi(u_3) &= 0.\end{aligned}$$

Resultaria llavors que tots són 0 i això contradiu que $\alpha \neq 0$. Per tant, sempre podem aplicar el cas anterior i seguir procedint en el canvi de base ortogonal. □

Definició 4.33. *Una isometria entre espais quadràtics (E_1, ϕ_1) i (E_2, ϕ_2) és una funció lineal $\tau : E_1 \to E_2$ tal que commuta de la següent manera:*

Si hi ha una funció lineal τ invertible que compleix el diagrama llavors diem que els espais quadràtics són isomètrics i les formes quadràtiques ϕ_1 i ϕ_2 són equivalents; $\phi_1 \sim \phi_2$.

El determinant de dues formes quadràtiques equivalents és el mateix. Per veure-ho ens ajudem del lema de Witt.



Teorema 4.34. *(Lema de Witt). Siguin $f_1(X_1,\ldots,X_m)$, $f_2(X_1,\ldots,X_m)$, $g_1(Y_1,\ldots,Y_n)$ i $g_1(Y_1,\ldots,Y_n)$ formes quadràtiques tal que f_1 i f_2 són regulars, $f_1 \sim f_2$ i $(f_1+g_1) \sim (f_2+g_2)$, llavors $g_1 \sim g_2$.*

Aquest teorema ens demostra que podem utilitzar l'eina de la cancel·lació quan busquem formes equivalents. La demostració del teorema la veurem més endavant. Abans hem de formar-nos en les isotropies en espais quadràtics.

Una isometria d'un espai quadràtic (E,ϕ) a si mateix rep el nom de autoisometria. Consisteix en una funció lineal τ que compleix $\phi \circ \tau = \phi$. Si tenim que (E,ϕ) és regular llavors el seu conjunt d'isometries són totes invertibles i formen un subgrup de $GL(U)$ anomenat $O_\phi(E)$.

Investiguem una mica aquest conjunt $O_\phi(E)$.

Proposició 4.35. *Una funció lineal $\tau \in O_\phi(E)$ compleix* $\det\tau = \pm 1$.

Demostració. Sigui $(u_1,\ldots,u_m)$ una base de E, considerem la matrius $S = (\psi(u_i,u_j))_{i,j}$. Si T és la matriu de τ en aquesta base llavors la matriu de $\phi\circ\tau$ és $T^tST = S$, per tant

$$\det(T^tST = S) = (\det T)^2 \cdot \det S = \det S.$$

El que implica que $\det T = \pm 1$. □

Considerem ara el subgrup de $O_\phi(E)$ definit per

$$O_\phi^+(E) := \{\tau \in O_\phi(E) | \det\tau = +1\}.$$

Tenim $|O_\phi(E) : O_\phi^+(E)| = 2$. Al haver-hi un sol element $\tau \in O_\phi(E)$ amb $\det\tau = -1$ (que n'hi ha), llavors l'index és immediatament 2.

Exemple 4.36. Prenem u tal que $\phi(u) \neq 0$. Passa que $E =< u > + < u >^\perp$, definim l'aplicació lineal τ_u:

$$\begin{aligned} \tau_u : & U \to U, \\ & u \mapsto -u \\ & v \mapsto v, \text{ per a tot } v \in < u >^\perp . \end{aligned}$$

Aquesta funció τ_u té determinant -1.

D'aquesta aplicació en diem reflexió respecte l'hiperplà ortogonal a $< u >$. Ve donada per la formula

$$\tau_u(v) = v - 2\frac{\psi(u,v)}{\psi(u,u)}u.$$

En particular, si $\phi(u) = \phi(v)$ i $\phi(u - v) \neq 0$, llavors

$$\tau_{u-v}(u) = v,\ \tau_{u-v}(v) = u.$$

El resultat s'aconsegueix substituint a partir de la formula anterior.

Proposició 4.37. *Si $u, v \in E$ compleixen $\phi(u) = \phi(v) \neq 0$, llavors existeix $\tau \in O_\phi(E)$ tal que $\tau(u) = v$.*

Demostració. Si $\phi(u - v) \neq 0$, llavors tenim la reflexió τ_{u-v}.

Si $\phi(u + v) \neq 0$, llavors $\tau_{u+v}(u) = -v$, i si composem aquesta reflexió amb τ_u, tenim $(\tau_u \circ \tau_{u+v})(u) = v$.

No poden ser les dues 0 a l'hora. Això implicaria

$$0 = \phi(u + v) + \phi(u - v) = 2\phi(u) + 2\phi(v) = 4\phi(v) \neq 0.$$

□

Si dim $E > 1$ llavors en la proposició anterior pot ser que agafem el producte de dues reflexions, per tant $\tau \in O^+_\phi(E)$. En aquest cas sabem que existeix $w \perp u$ tal que $\phi(w) \neq 0$, per tant $(\tau_{u-v} \circ \tau_w)(u) = v$ si $\phi(u - v) \neq 0$, ja que $\tau_w(u) = u$. I en cas que $\phi(u + v) \neq 0$ seguim tenint, com abans, $(\tau_u \circ \tau_{u-v})(u) = v$.

Teorema 4.38. *Siguin $V_1, V_2 \subseteq E$ subespais regulars de E isomètrics per una isometria $\tau : V_1 \to V_2$, llavors la isometria pot ser extesa a una autoisometria a tot E.*

Demostració. Al ser V_1 regular existeix $v_1 \in V_1$ tal que $\phi(v_1) \neq 0$. Per tant, ara tenim que $v_1 \in V_1$ i $\tau(v_1) \in V_2$. Per la proposició anterior sabem que hi ha $\sigma \in O_\phi(E)$ tal que $\sigma(\tau(v_1)) = v_1$. Per tant, substituïm ara V_2 per σV_2 i τ per $\sigma\tau$, tal que $v_1 \in V_1 \cap V_2$ i $\tau(v_1) = v_1$.

Si dim $V_1 = 1$ ja hem acabat. Per la resta fem inducció sobre la dimensió. Considerem:

$$E' :=< v_1 >^\perp,\ V_1' = E' \cap V_1,\ V_2' = E' \cap V_2.$$

Tenim dim V_1' =dim $V_1 - 1$, dimV_2' = dim $V_2 - 1$ i $pV_1' = V_2'$. Per la hipòtesi d'inducció, hi ha una autoisometria τ' de E' tal que $\tau|_{V_1} = \tau$. Podem definir ja l'autoisometria a tot E com:

$$\begin{aligned} \sigma :& U \to U, \\ & v \mapsto v, \\ & u \mapsto \tau'(u). \end{aligned}$$

□

Proposició 4.39. *Siguin E_1 i E_2 espais quadràtics isomètrics i $V_1 \subseteq E_1$ i $V_2 \subseteq E_2$ subespais isomètrics i regulars. Llavors $V_1^\perp$ i $V_2^\perp$ són isomètrics.*

Demostració. Per hipòtesis existeix una isometria τ de E_1 a E_2. Podem intercanviar E_1 per τE_1 i V_1 per τV_1 per poder assumir que $(E_1, \phi_1) = (E_2, \phi_2)$ són un únic espai quadràtic (E, ϕ) i V_1 i V_2 són subespais regulars i isomètrics via un $\rho : V_1 \to V_2$. Llavors, per la proposició anterior sabem que podem estendre aquesta funció ρ a una funció σ de tot E. I llavors $\sigma V_1 = V_2$ i $\sigma V_1^\perp = V_2^\perp$. □

Aquest teorema demostra el lema de Witt. Ja que, tenint formes quadràtiques

$$f_1(X_1, \ldots, X_m) + g_1(Y_1, \ldots, Y_n) \sim f_2(X_1, \ldots, X_m) + g_2(Y_1, \ldots, Y_n),$$

amb f_1, f_2 regulars i equivalents, considerem l'espai quadràtic E_1 amb forma quadràtica $f_1(X) + g_1(Y)$, i un E_2 amb forma quadràtica $f_2(X) + g_2(Y)$, llavors f_1 i f_2 corresponen a subespais regulars isomètrics $V_1 \subset E$ i $V_2 \subset E$. Les formes quadràtiques g_1 i g_2 corresponen als espais quadràtics $V_1^\perp$ i $V_2^\perp$ que són isomètrics també.

4.3 Formes quadràtiques a $\mathbb{Q}_p$

Volem veure quan les formes quadràtiques tenen arrels diferents de zero a $\mathbb{Q}_p$. Tenim una primera proposició que ens acota considerablement els casos a estudiar.

Proposició 4.40. *Suposem $p > 2$ primer finit i ϕ una forma quadràtica regular en $\mathbb{Q}_p$.*

1. *Per a dimensió ≥ 3 si ϕ té una forma diagonal*

$$\phi = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \alpha_3 X_3^2 + \ldots$$

essent $\alpha_1, \alpha_2, \alpha_3$ unitats, llavors ϕ és isotròpic.

2. *Qualsevol forma quadràtica de dimensió ≥ 5 és isotròpica.*

És important veure que $p \neq 2$ ja que en el primer cas per $p = 2$ és fals. Més endavant en veurem un contraexemple. La segona en canvi és certa i més tard ho veurem.

Demostració.

1. Per un cos finit qualsevol forma quadràtica de dimensió ≥ 3 és isotròpica. Per tant, això ens diu que existeix un vector $a = (a_1, a_2, a_3)$ de elements de $\mathbb{Z}/p\mathbb{Z}$ tal que $a \neq 0$ i $\phi(a) = 0$. Això afegit a que $\phi'_{X_1}(a) = 2a \neq 0$, fa que qualsevol element $X_0 = (x_1, x_2, x_3) \equiv (a_1, a_2, a_3) \pmod{p}$ serveix com a primera aproximació per aplicar el lema de Hensel i veure que existeix una solució $X \in \mathbb{Z}_p^3$ i, per tant, ϕ és isotròpica.

2. Assumim $n = 5$ i que $\phi = \alpha_1 X_1^2 + \ldots + \alpha_5 X_5^2$. Amb canvis de variables veiem que podem suposar que $ord_p(\alpha_i) = 0, 1$ per tots els coeficients. En aquest cas $\phi = \phi_1 + p\phi_2$, on ϕ_1 i ϕ_2 són formes quadràtiques on tots els seus coeficients són unitats. Alguna de les dues formes quadràtiques ha de tenir dimensió ≥ 3. Per tant, alguna de les dues formes serà isotròpica, així doncs la forma ϕ és isotròpica.

□

5 Símbol de Hilbert

Definició 5.1. *Per un parell a, b d'elements de $\mathbb{Q}_p$, el símbol de Hilbert és una aplicació definida com:*

$$(a,b)_p = \begin{cases} +1, & \text{si } aX^2+bY^2-Z^2 \text{ és isotròpica,} \\ -1, & \text{si } aX^2+bY^2-Z^2 \text{ no és isotròpica.} \end{cases}$$

Com hem vist en la proposició 4.29, $aX^2+bY^2-Z^2$ és isotròpica si i només si Z^2-aX^2 representa b.

Veiem algunes propietats bàsiques del símbol de Hilbert:

1. $(a,b)_p = (b,a)_p$.
2. $(a,-a)_p = 1$, observem que $(1,1,0) = (X,Y,Z)$ és arrel de $aX^2 - aY^2 - Z^2$.
3. $(a,1)_p = 1$ ja que $(X,Y,Z) = (0,1,1)$ és solució de $aX^2 + Y^2 - Z^2$.
4. $(a,\gamma^2 b)_p = (a,b)_p$ ja que podem fer un canvi de variable $Y' = Y/\gamma$.
5. $(a,\gamma^2) = 1$.

Hi ha una manera equivalent de definir el simbol de Hilbert, que entre altres ens servirà per demostrar proposicions més endavant.

Proposició 5.2. $(a,b)_p = 1 \Leftrightarrow b$ *és la norma d'algun element a* $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$.

Demostració. Si a és un quadrat llavors él símbol és sempre 1, però si no és un quadrat llavors és diferent. Per un element arbitrari $z + x\sqrt{a} \in \mathbb{Q}_p(\sqrt{a})^*$ calculem que té norma $z^2 - ax^2$. Així doncs és equivalent a exigir que b sigui representat per $Z^2 - aX^2$.
□

El simbol de Hilbert encara té més propietats però aquestes necessiten una demostració més amplia. En aquest tema les veurem.

Proposició 5.3. *El símbol de Hilbert és multiplicatiu respecte cada variable:*

$$(a, b_1b_2)_p = (a,b_1)_p \cdot (a,b_2)_p$$
$$(a_1a_2, b)_p = (a_1,b)_p \cdot (a_2,b)_p.$$

Ho demostrarem amb una altra proposició:

Proposició 5.4. *Per un a fix, el conjunt $G_a := \{b | (a,b) = 1\}$ és un subgrup de $\mathbb{Q}_p^*$ d'índex 1 ó 2.*

Si demostrem aquesta proposició immediatament queda demostrada l'anterior. Si suposem que G_a és un grup d'índex 1 o 2 tenim 3 casos:

1. $b_1, b_2 \in G_a$. Llavors $(a,b_1)_p \cdot (a,b_2)_p = (a,b_1b_2)_p = 1$, al ser G_a subgrup.

2. $b_1 \in G_a$ i $b_2 \notin G_a$. Llavors $(a, b_1) = 1$ i $(a, b_2) = (a, b_1 b_2) = -1$.

3. $b_1, b_2 \notin G_a$. Llavors al tenir G_a index ≤ 2, llavors $(a, b_1 b_2) = 1$.

De fet tenim demostracions encara més explícites per la propietat 1 i 2:
Per a 1, tenim que si $Z^2 - aX^2$ representa a b_1 i b_2 llavors representa a $b_1 b_2$. Això es conseqüència que si tenim $z_1^2 - ax_1^2 = b_1$ i $z_2^2 - ax_2^2 = b_2$, $(Z, X) = (z_1 z_2 + a x_1 x_2, x_2 z_1 + x_1 z_2)$ és solució:

$$\begin{aligned}(z_1 z_2 + a x_1 x_2)^2 + a(x_2 z_1 + x_1 z_2)^2 =& (z_1 z_2)^2 + 2 z_1 z_2 a x_1 x_2 + (a x_1 x_2)^2 \\ & - a((x_2 z_1)^2 + 2 z_1 z_2 x_1 x_2 + (x_1 z_2)^2) \\ =& (z_1 z_2)^2 + (a x_1 x_2)^2 - a((x_2 z_1)^2 + (x_1 z_2)^2) \\ =& z_1^2 z_2^2 + a^2 x_1^2 x_2^2 - a x_2^2 z_1^2 - a x_1^2 z_2^2 \\ =& (z_1^2 - a x_1^2) \cdot (z_2^2 - a x_2^2) = b_1 \cdot b_2.\end{aligned}$$

Per a 2 només hem de veure que si $(a, b_1)_p = 1$ i $(a, b_1 b_2)_p = 1$, llavors $(a, b_2)_p$ no pot ser -1, ja que

$$(a, b_2)_p = (a, b_2 b_1^2)_p = (a, b_1) \cdot (a, b_1 b_2) = 1 \cdot 1 = 1.$$

La tercera en canvi es preveu més complicada.

Demostració. (de la proposició (5.4)). Si $a \in (\mathbb{Q}_p^*)^2$ llavors $(a, b)_p = 1$ per tot $b \in \mathbb{Q}_p$ per tant és un subgrup d'índex 1.

Veiem que passa si $a \notin (\mathbb{Q}_p^*)^2$. En aquest cas, $|\mathbb{Q}_p(\sqrt{(a)})^* : \mathbb{Q}_p^*| = 2$. La norma $N_{\mathbb{Q}_p(\sqrt{(a)})/\mathbb{Q}_p}$ és un homeomorfisme $\mathbb{Q}_p(\sqrt{(a)})^* \to \mathbb{Q}_p^*$, així queda clar que la seva imatge, que és G_a, és un subgrup en $\mathbb{Q}_p^*$. Volem veure ara que el seu índex és 1 ó 2.

Hem vist abans que $(\mathbb{Q}_p^*)^2 \subseteq G_a$, per tant l'índex $|\mathbb{Q}_p^* : G_a|$ ha de dividir $|\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2|$. Que recordem que val:

$$|\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2| = \begin{cases} 2, & \text{si } p = \infty, \\ 4, & \text{si } 2 < p < \infty. \\ 8, & \text{si } p = 2. \end{cases}$$

En el cas $p = \infty$ ja hem acabat. L'índex del subgrup G_a divideix 2, per tant és 1 ó 2. Per $2 < p < \infty$ hem de veure només que existeix $b \in G_a$ però al mateix temps $b \notin (\mathbb{Q}_p^*)^2$. Veiem que existeix $c \in \mathbb{Q}_p$ però que no pertany a G_a, llavors podrem afirmar que $|\mathbb{Q}_p^* : G_a| = 2$. Estudiem els casos que a té ordre p-àdic 1 ó 0.

Si suposem $ord_p(a) = 0$, llavors per tot b amb $ord_p(b) = 0$ la forma quadràtica $aX^2 + bY^2 - Z^2$ és isotròpica al ser unitats tots els coeficients, així que $\mathbb{Z}_p \subseteq G_a$. En canvi, no totes les unitats són quadrats. I també veiem que $aX^2 + pY^2 - Z^2$ no és isotròpica. Per tant, tenim un element que pertany a G_a i no a $(\mathbb{Q}_p^*)^2$ (qualsevol unitat que no sigui quadrat), i també tenim un element que pertany a $\mathbb{Q}_p^*$ i no a G_a, que és p.

Si suposem $ord_p(a) = 1$, llavors $a = p \cdot \mu$, on $\mu \in \mathbb{Z}_p$. Si escollim un element γ que sigui unitat i no sigui quadrat tenim que $p\mu X^2 + \gamma Y^2 - Z^2$ és no isotròpica i $\gamma \notin G_a$.

Sinò $\gamma Y^2 - Z^2$ seria isotròpica i aixo no pot ser ja que γ no és un quadrat.

Així concloem que $|\mathbb{Q}_p^* : G_a| = 2$ per p primer finit diferent de 2. Amb un raonament similar arribaríem a la conclusió que $|\mathbb{Q}_p^* : G_a| = 2$ per $p = 2$. □

Veiem exemples de símbol de Hilbert. En el cas $p = \infty$, és a dir, en els reals, $aX^2 + bY^2 - Z^2$ és isotròpica si i només si $a, b < 0$.

$$(a,b)_p = \begin{cases} \text{-1}, & \text{si } a,b<0, \\ +1, & \text{per la resta de casos,} \end{cases}$$

Ara per $2 < p < \infty$ veiem alguns casos:

Exemple 5.5. 1. Per a, b unitats $aX^2 + bY^2 - Z^2$ és isotròpic i $(a,b)_p = 1$.

2. Per a unitat $(a,p)_p = (\frac{a}{p})$ és equivalent al símbol de Legendre. ($aX^2 + pY^2 - Z^2$ isotròpic si i només si $aX^2 - Z^2$ isotròpic.)

3. $(p,p)_p = (p,-p)_p \cdot (p,-1)_p = 1 \cdot (-1,p)_p = (\frac{-1}{p})$.

4. $(p\mu,\mu)_p = (p,\mu)_p \cdot (\mu,\mu)_p = (p,\mu)_p = (\frac{\mu}{p}) = -1$, al no ser μ un quadrat.

5. $(p\mu,p)_p = (p,p)_p \cdot (\mu,p)_p = -(p,p)_p = -(\frac{-1}{p})$.

6. $(p\mu,p\mu)_p = (p,p\mu)_p \cdot (\mu,p\mu)_p = (\frac{-1}{p})$.

Ja tenim resumits tots els casos possibles de símbol de Hilbert en funció del símbol de Legendre $(\frac{-1}{p})$. Així doncs val la pena recordar que:

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ \text{-1}, & p \equiv 3 \pmod 4. \end{cases}$$

Per a $p = 2$, recordem que $\mathbb{Z}_2^*/(\mathbb{Z}_2^*)^2$ pot ser identificat amb $(\mathbb{Z}/8\mathbb{Z})^*$, que està representat pels elements $\{1,3,5,7\}$. El grup $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ està representat per $\{1,2,3,5,6,7,10,14\}$, els residus i el seu valor multiplicat per 2. Investiguem el valor del seu símbol de Hilbert i obtenim:

$\mathbb{Q}_2$	1	3	5	7	2	6	10	14
1	+1	+1	+1	+1	+1	+1	+1	+1
3	+1	−1	+1	−1	−1	+1	−1	+1
5	+1	+1	+1	+1	−1	−1	−1	−1
7	+1	−1	+1	−1	+1	−1	+1	−1
2	+1	−1	−1	+1	+1	−1	−1	+1
6	+1	+1	−1	−1	−1	−1	+1	+1
10	+1	−1	−1	+1	−1	+1	+1	−1
14	+1	+1	−1	−1	+1	+1	−1	−1

Per entendre com hem arribat a aquests valors són necessaris conceptes que estudiarem més avall.

5.1 Producte de Hilbert

Fixats $a, b \in \mathbb{Q}^*$. Observem que $(a,b)_p = 1$ per tot primer excepte per un conjunt finit de p ja que si $p > 2$ i $a, b \in \mathbb{Z}_p^*$ llavors $(a,b)_p = 1$. Per tant, el següent producte està ben definit.

Teorema 5.6. *(Fórmula del producte). Per $a, b \in \mathbb{Q}^*$ tenim*

$$\prod_{2 \leq p \leq \infty} (a,b)_p = 1.$$

O, el que és el mateix, $(a,b)_p$ és -1 per un nombre parell de p's.

Exemple 5.7. Fixem $(10,14)_p$. Calculem:

$$\begin{aligned}
(10,14)_2 &= -1 \\
(10,14)_3 &= 1, \\
(10,14)_5 &= (2,14)_5 \cdot (5,14)_5 = 1 \cdot (\frac{14}{5}) = 1 \cdot (\frac{-1}{5}) = 1 \cdot 1 = 1, \\
(10,14)_7 &= (10,2)_7 \cdot (10,7)_7 = 1 \cdot (\frac{10}{7}) = 1 \cdot (\frac{3}{7}) = 1 \cdot (-1) = -1, \\
(10,14)_{11} &= 1, \\
(10,14)_{13} &= 1, \\
&\dots \\
(10,14)_\infty &= 1.
\end{aligned}$$

Observació 5.8. Del teorema anterior n'observem que llavors sigui ϕ una forma quadràtica ternària en $\mathbb{Q}$. Llavors el conjunt

$$\{p | \phi \text{ és no isotròpic sobre } \mathbb{Q}_p\}$$

és finit i té cardinalitat parella, ja que ϕ no és regular sempre és isotròpica, i si ho és, ϕ té forma $aX^2 + bY^2 - Z^2$, i això no és isotròpic si i només si $(a,b)_p = -1$.

Procedim ara doncs amb la demostració del teorema (5.6).

Demostració. Només considerem uns quants casos ja que el símbol de Hilbert és multiplicatiu:

- $a = -1$, $b = -1$,
- $a = -1$, $b = 2$,
- $a = -1$, $b = q$ un primer imparell,
- $a = 2$, $b = 2$,
- $a = 2$, $b = q$,
- $a = q$, $b = q$,
- $a = q$, $b = q'$, on $q \neq q'$.

1. El primer cas, $a = -1$ i $b = -1$, per p finit diferent de 2, tenim que -1 sempre és unitat. Per tant, al ser els tres coeficients unitaris tenim que $(a, b)_p = 1$. Per a $p = \infty$ tenim $(-1, -1)_\infty = -1$.
Ara només queda veure quan val $(-1, -1)_2$. Volem veure que $-X^2 - Y^2 - Z^2$ és no-isotròpica, de ser-ho $x^2 + y^2 + z^2$ tindria solució en $\mathbb{Z}_2^*$. Podem assumir que $\text{mcd}(x, y, z) = 1$. Suposem que x, y són imparells i z parell però llavors $x^2+y^2+z^2 \equiv 2 \pmod 4$. Contradicció. Per tant,

$$\prod_{2 \leq p \leq \infty} (-1, -1)_p = (-1, -1)_2 \cdot (-1, -1)_\infty = 1.$$

A continuació ens desviem una mica per veure quan les formes quadràtiques ternàries són isotròpiques a $\mathbb{Q}_2^*$. Acabem de veure que el fet de tenir tres unitats com a coeficients no és suficient per a que sigui isotròpica.

Si ϕ té la forma $\alpha X^2+\beta Y^2+\gamma Z^2$ podem assumir $ord_2(\alpha), ord_2(\beta), ord_2(\gamma) \in \{0, 1\}$. Tenim 2 casos, tots tres coeficients són unitats, o un té ordre 1:

- Si α, β, γ són unitats i suposem que existeix una solució (x, y, z). Per aritmètica bàsica dos dels coeficients han de ser imparells i un parell, si els elements imparells són x, y llavors els seus coeficients han de complir $\alpha+\beta \equiv 0 \pmod 4$. Anàlogament podria passar per els parells β, γ i α, γ, el que ens porta a:

$$\phi \text{ isotròpica } \Leftrightarrow \begin{cases} \alpha + \beta \equiv 0 \pmod 4, \\ \text{ ó} \\ \alpha + \gamma \equiv 0 \pmod 4, \\ \text{ ó} \\ \beta + \gamma \equiv 0 \pmod 4. \end{cases}$$

  La primera implicació l'hem explicat, l'altra ($\Leftarrow$), és una conseqüència del lema de Hensel generalitzat. Si tenim que, per exemple, $\alpha + \beta \equiv 0 \pmod 4$, llavors o bé $\alpha + \beta \equiv 0 \pmod 8$ o bé $\alpha + \beta \equiv 4 \pmod 8$.
  Si es dona el primer cas tenim que $\phi(1, 1, 0) \equiv 0 \pmod 8$ i $\phi'_X(1, 1, 0) \not\equiv 0 \pmod 4$. Similarment, en el segon cas tenim que $\phi(1, 1, 2) \equiv 0 \pmod 8$ i $\phi'_X(1, 1, 2) \not\equiv 0 \pmod 4$. En qualsevol cas tenim ua aproximació correcta per aplicar el lema de Hensel i obtenir una solució.

- Si α, β són unitats i γ no, anàlogament veuríem que:

$$\phi \text{ isotròpica } \Leftrightarrow \begin{cases} \alpha + \beta \equiv 0 \pmod 8, \\ \text{ ó} \\ \alpha + \beta + \gamma \equiv 0 \pmod 8. \end{cases}$$

Seguim ara amb els casos un cop hem après a discernir entre formes isotròpiques i formes no-isotròpiques en $\mathbb{Q}_2^*$.

2. El segon cas, $a = -1$ i $b = 2$, és senzill. Per p finit diferent de 2 $(-1, 2)_p = 1$. En cas que $p = 2$ tenim que $-1 + 2 - 1 \equiv 0 \pmod 8$ per tant ϕ és isotròpica, i per $p = \infty$, tenim $(-1, 2)_\infty = 1$.

3. En el tercer cas $a = -1$ i $b = q$ un primer imparell, per a tot $p \neq q$ passa que la forma $-X^2 + qY^2 - Z^2$ és isotròpica. Per $p = q$ tenim que és isotròpica si i només si $X^2 + Z^2$ és isotròpica si i només si -1 és un quadrat mòdul q. Sobre $\mathbb{R}$ és isotròpica i sobre $\mathbb{Q}_2$ és isotròpica si i només si $q \equiv 1 \pmod 4$ que és equivalent a que -1 sigui quadrat modul q. Per tant, o bé les és isotròpica en $\mathbb{Q}_2$ i en $\mathbb{Q}_q$ o bé no ho és en cap de les dues.
   El cas $a = 2$ i $b = q$ és pot comprovar anàlogament.

4. En el cinquè cas tenim que $a = q$ i $b = q' \neq q$. Per qualsevol $p \neq q, q'$ la forma $qX^2 + q'Y^2 - Z^2$ és isotròpica. Per $\mathbb{Q}_2$ és isotròpica si i només si es compleix alguna de les següents condicions:

$$q + q' \equiv 0 \pmod 4, \text{ o bé } q - 1 \equiv 0 \pmod 4, \text{ ó } q' - 1 \equiv 0 \pmod 4.$$

   La primera equivalència només es donarà si es dona alguna de les altres dues, per tant, no cal tenir-la en compte. En qualsevol cas, $(q, q')_2 = (-1)^{\frac{q-1}{2}\frac{q'-1}{2}}$.
   Finalment, veiem que $qX^2 + q'Y^2 - Z^2$ és isotròpic sobre $\mathbb{Q}_q$ si i només si $q'Y^2 - Z^2$, per tant,

$$(q, q')_q = (\frac{q}{q'}),\ (q, q')_{q'} = (\frac{q'}{q}),$$

   i passa que

$$\prod_{2 \leq p \leq \infty} (q, q')_p = (-1)^{\frac{q-1}{2}\frac{q'-1}{2}} \cdot (\frac{q}{q'}) \cdot (\frac{q'}{q}).$$

   que substituint qualsevol dels dos símbols de Legendre veiem que és 1.

□

6 L'invariant de Hasse

Estem a punt de descobrir el tercer invariant de les formes quadràtiques. Hem vist la dimensió (nombre de variables de la forma quadràtica ϕ), el determinant $\delta(\phi) \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ i ara l'invariant Hasse.

Sigui ϕ una forma quadràtica escrita en la forma diagonal

$$\phi = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \ldots + \alpha_m X_m^2.$$

Definim l'invariant de Hasse com

$$c(\phi) = \prod_{1 \leq i < j \leq m} (\alpha_i, \alpha_j)_p.$$

Demostrarem que l'invariant de Hasse és invariant.

Teorema 6.1. *L'invariant de Hasse no depèn de la diagonalització de ϕ.*

Ho demostrarem més endavant. De moment però, veurem que ser ϕ isotròpica o no ser-ho queda únicament determinat pels tres invariants.

Teorema 6.2. *Sigui p qualsevol primer finit. Si tenim que ϕ és una forma quadràtica en $\mathbb{Q}_p$ de n variables, llavors:*

1. *Si n=2, llavors ϕ és isotròpica si i només si $\delta(\phi) = -1$ en $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, bàsicament quan $-\delta(\phi)$ és un quadrat.*
2. *Si $n = 3$, llavors ϕ és isotròpica si i només si $c(\phi) = (-1, -\delta(\phi))_p$.*
3. *Si $n = 4$, llavors ϕ és no isotròpica si i només si $c(\phi) = (-1, -1)_p$ i $\delta(\phi) \in (\mathbb{Q}_p^*)^2$.*
4. *Si $n \geq 5$, llavors ϕ és sempre isotròpic.*

El demostrarem posteriorment.

Lema 6.3. *Sigui ϕ una forma regular binària, llavors ϕ és isotròpica si i només si $\delta(\phi) = -1$ en $K^*/(K^*)^2$.*

Demostració. Considerem $\phi = \alpha X^2 + \beta Y^2$. Llavors $\delta(\phi) = \alpha\beta$. Veiem que ϕ és isotròpic si i només si $\alpha\phi$ ho és, i $\alpha\phi$ és equivalent a $X^2 + \delta(\phi)Y^2$, que és isotròpic si i només si $-\delta(\phi)$ és quadrat. □

Lema 6.4. *Sigui ϕ una forma binaria en $\mathbb{Q}_p$, llavors existeix $\epsilon(\phi) \in \{-1, 1\}$ tal que:*

$$\beta \in \mathbb{Q}_p \text{ està representat per } \phi \Leftrightarrow (\beta, -\delta(\phi))_p = \epsilon.$$

Demostració. Assumim que $\phi = \alpha_1 X_1^2 + \alpha_2 X_2^2$ està en forma diagonal. Llavors β està representat per ϕ si i només si $\phi - \beta Y^2$ és isotròpica si i només si el símbol de Hilbert de $\frac{\alpha_1}{\beta}X^2 + \frac{\alpha_2}{\beta}Y^2 - Z^2$ és 1.

$$(\frac{\alpha_1}{\beta}, \frac{\alpha_2}{\beta})_p = (\alpha_1, \alpha_2)_p \cdot (\alpha_1, \frac{1}{\beta})_p \cdot (\frac{1}{\beta}, \alpha_2)_p \cdot (\frac{1}{\beta}, \frac{1}{\beta})_p.$$

Com que $(1/\beta, \mu)_p \cdot (\beta, \mu) = 1$ podem substituir $1/\beta$ per β.

$$(\frac{\alpha_1}{\beta}, \frac{\alpha_2}{\beta})_p = (\alpha_1, \alpha_2)_p \cdot (\alpha_1, \beta)_p \cdot (\beta, \alpha_2)_p \cdot (\beta, \beta)_p.$$

Sabem que $(\beta, \beta)_p = (\beta, -1)_p$,

$$\begin{aligned}(\frac{\alpha_1}{\beta}, \frac{\alpha_2}{\beta})_p &= (\alpha_1, \alpha_2)_p \cdot (\alpha_1, \beta)_p \cdot (\beta, \alpha_2)_p \cdot (\beta, -1)_p, \\ &= (\alpha_1, \alpha_2)_p \cdot (\alpha_1\alpha_2, \beta^2)_p \cdot (\beta, -1)_p, \\ &= (\alpha_1, \alpha_2)_p \cdot (-\alpha_1\alpha_2, \beta)_p.\end{aligned}$$

Per tant, hem vist que β està representat si i només si $(\alpha_1, \alpha_2)_p = (-\delta(\phi), \beta)_p$. La funció $\epsilon(\phi)$ que buscàvem era $(\alpha_1, \alpha_2)_p$. □

Observació 6.5. En aquesta demostració hem vist que $(\alpha_1, \alpha_2)_p$ és invariant en formes binàries. Tenim doncs, que $c(\phi)$ està ben definit per formes binàries i que el l'ϵ que buscàvem era en realitat $c(\phi)$.

Ja podem demostrar que l'invariant de Hasse està ben definit.

Demostració. (del teorema (6)). Volem veure que si tenim dos formes $\phi = \alpha_1 X_1^2 + \ldots + \alpha_m X_m^2$ i $\omega = \beta_1 X_1^2 + \ldots + \beta_m X_m^2$ equivalents llavors:

$$\prod_{1\leq i<j\leq m} (\alpha_i, \alpha_j)_p = \prod_{1\leq i<j\leq m} (\beta_i, \beta_j)_p.$$

Per la proposició (4.32) podem assumir que $\alpha_i = \beta_i$ és igual per totes les i menys com a màxim dues.

$$\phi = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \alpha_3 X_3^2 + \ldots + \alpha_m X_m^2,$$
$$\omega = \beta_1 X_1^2 + \beta_2 X_2^2 + \alpha_3 X_3^2 + \ldots + \alpha_m X_m^2.$$

Per el teorema de Witt tenim que si $\phi \sim \omega$ i, òbviament, $\phi - \alpha_1 X_1^2 + \alpha_2 X_2^2 \sim \omega - \beta_1 X_1^2 + \beta_2 X_2^2$, llavors

$$\alpha_1 X_1^2 + \alpha_2 X_2^2 \sim \beta_1 X_1^2 + \beta_2 X_2^2.$$

Per la demostració del lema anterior sabem que si són formes binàries equivalents llavors $(\alpha_1, \alpha_2)_p = (\beta_1, \beta_2)_p$, és més, $\alpha_1\alpha_2 = \beta_1\beta_2$ mòdul $(\mathbb{Q}_p^*)^2$. Així doncs,

$$\begin{aligned}\prod_{1\leq i<j\leq m} (\alpha_i, \alpha_j)_p &= (\alpha_1, \alpha_2)_p \cdot \prod_{3\leq j\leq m} (\alpha_1\alpha_2, \alpha_j)_p \cdot \prod_{3\leq i<j\leq m} (\alpha_i, \alpha_j)_p \\ &= (\beta_1, \beta_2)_p \cdot \prod_{3\leq j\leq m} (\beta_1\beta_2, \beta_j)_p \cdot \prod_{3\leq i<j\leq m} (\beta_i, \beta_j)_p = \prod_{1\leq i<j\leq m} (\beta_i, \beta_j)_p.\end{aligned}$$

□

Lema 6.6. *Siguin $\phi(X) = \phi(X_1, \ldots, X_m)$ i $\omega(Y) = \omega(Y_1, \ldots, Y_n)$ formes quadràtiques, la seva suma $\phi(X) + \omega(Y)$, (una forma quadràtica de $n + m$ variables) compleix:*

- $\dim(\phi + \omega) = \dim \phi + \dim \omega$,
- $\delta(\phi + \omega) = \delta(\phi) \cdot \delta(\omega)$,
- $c(\phi + \omega) = c(\phi) \cdot c(\omega) \cdot (\delta(\phi), \delta(\omega))_p$.

Demostració. La primera és obvia i la segona si ens imaginem les dues formes quadràtiques en la forma diagonal també és bastant evident. La última necessita més explicació. Suposem que les formes ϕ i ω estan en forma diagonal $\alpha_1 X_1^2 + \ldots + \alpha_m X_m^2$ i $\beta_1 X_1^2 + \ldots + \beta_m X_m^2$, llavors,

$$\begin{aligned}c(\phi + \omega) &= \prod_{1\leq i<j\leq m} (\alpha_i, \alpha_j)_p \cdot \prod_{1\leq i<j\leq n} (\beta_i, \beta_j)_p \cdot \prod_{1\leq j\leq n}^{1\leq i\leq m} (\alpha_i, \beta_j)_p \\ &= c(\phi) \cdot c(\omega) \cdot \prod_{1\leq j\leq n} (\alpha_1\alpha_2 \ldots \alpha_m, \beta_j)_p \\ &= c(\phi) \cdot c(\omega) \cdot (\alpha_1\alpha_2 \ldots \alpha_m, \beta_1\beta_2 \ldots \beta_n)_p \\ &= c(\phi) \cdot c(\omega) \cdot (\delta(\phi), \delta(\omega))_p.\end{aligned}$$

□

Ara tornem al teorema 6.2 per demostrar-lo finalment.

Demostració. 1. Si n=2, llavors ϕ és isotròpica si i només si $\delta(\phi) = -1$ en $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. Ho hem vist en la demostració del lema (6.4).

2. Si $n = 3$, llavors ϕ és isotròpica si i només si $c(\phi) = (-1, -\delta(\phi))_p$.
Escrivim ϕ en la seva forma diagonal $\alpha_1 X_1^2 + \alpha_2 X_2^2 + \alpha_3$, isotròpica si i només si $\frac{\alpha_1}{-\alpha_3} X_1^2 + \frac{\alpha_2}{-\alpha_3} + X_2^2 - X^3$ isotròpica. Per tant, és isotròpica si i només si el seu símbol de Hilbert és 1. Veiem llavors la relació entre aquest i el invariant de Hasse:

$$c(\phi) = (\frac{\alpha_1}{-\alpha_3}, \frac{\alpha_2}{-\alpha_3})_p \cdot (\frac{\alpha_1}{-\alpha_3}, -1)_p \cdot (\frac{\alpha_2}{-\alpha_3}, -1)_p = (\frac{\alpha_1}{-\alpha_3}, \frac{\alpha_2}{-\alpha_3})_p \cdot (-1 - \delta(\phi))_p.$$

3. Si $n = 4$, llavors ϕ és no isotròpica si i només si $c(\phi) = (-1, -1)_p$ i $\delta(\phi) \in (\mathbb{Q}_p^*)^2$.
Per demostrar aquest cas hem de visualitzar ϕ com la resta de dues formes quadràtiques binàries $\phi = f(X_1, X_2) - g(Y_1, Y_2)$. Per tant, $f = \alpha_1 X_1^2 + \alpha_2 X_2^2$ i $g = \beta_1 Y_1^2 + \beta_2 Y_2^2$.

Volem que ϕ sigui no-isotròpica. Per tant, ens hem d'assegurar que f i g son isotròpiques i no representen un mateix $\gamma \in \mathbb{Q}_p$.
El ser formes binàries no-isotròpiques equival a que

$$-\alpha_1\alpha_2 \notin (\mathbb{Q}_p^*)^2, \text{ i } -\beta_1\beta_2 \notin (\mathbb{Q}_p^*)^2.$$

El no representar un mateix element γ equival a que no existeix γ tal que:

$$\begin{aligned} c(f) = (\alpha_1, \alpha_2)_p = (\gamma, -\alpha_1\alpha_2)_p, \\ c(g) = (\beta_1, \beta_2)_p = (\gamma, -\beta_1\beta_2)_p. \end{aligned}$$

Per el lema 6.4.
Com que $-\alpha_1\alpha_2$i $-\beta_1\beta_2$ no són quadrats, llavors $(\gamma, -\alpha_1\alpha_2)_p$ i $(\gamma, -\beta_1\beta_2)_p$ són funcions no constants. De fet, per a la meitat d'elements té valor -1 i per l'altra 1. Si volem que $c(f)$ i $c(g)$ no coincideixin haurien de ser disjuntes. Això és equivalent a:

$$\begin{aligned} \alpha_1\alpha_2 = \beta_1\beta_2 \pmod{(\mathbb{Q}_p^*)^2} \\ (\alpha_1, \alpha_2)_p = (\beta_1, \beta_2)_p. \end{aligned}$$

Aquestes condicions són equivalents a dir que:

$$\begin{aligned} \delta(\phi) = \alpha_1\alpha_2\beta_1\beta_2 \in (\mathbb{Q}_p^*)^2, \\ c(\phi) = -(-1, -1)_p. \end{aligned}$$

La segona igualtat prové de utilitzar propietats del símbol de Hilbert:

$$\begin{aligned} c(\phi) &= (\alpha_1, \alpha_2)_p \cdot (-\beta_1, -\beta_2)_p \cdot (\alpha_1\alpha_2, \beta_1\beta_2)_p \\ &= (\alpha_1, \alpha_2)_p \cdot (-\beta_1, -\beta_2)_p \cdot (\alpha_1\alpha_2, \beta_1\beta_2)_p \\ &= (\alpha_1, \alpha_2)_p \cdot (\beta_1, \beta_2)_p \cdot (\beta_1, -1)_p \cdot (-1, -\beta_2)_p \cdot (\beta_1\beta_2, \beta_1\beta_2)_p \\ &= (-1) \cdot (\beta_1, -1)_p \cdot (-1, -\beta_2)_p \cdot (\beta_1\beta_2, \beta_1\beta_2)_p \\ &= -(-1, -\beta_1\beta_2)_p \cdot (\beta_1\beta_2, \beta_1\beta_2)_p \\ &= -(-1, \beta_1\beta_2)_p \cdot (-1, -1)_p \cdot (\beta_1\beta_2, \beta_1\beta_2)_p \\ &= -(-\beta_1\beta_2, \beta_1\beta_2)_p \cdot (-1, -1)_p = -(-1, -1)_p. \end{aligned}$$

4. Si $n \geq 5$, llavors ϕ és sempre isotròpic.
   Aquest cas ja el vam demostrar en la proposició per 4.40 per cosos K amb caràcter major a 2. Ara veurem una demostració transversal per a qualsevol valor de caràcter. Primer introduïm una nova proposició:

   Proposició 6.7. *Sigui ϕ una forma ternària regular, sabem que aquesta representa totes les classes mòdul quadrat en $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ menys com a màxim una.*

   Demostració. Sigui $\phi(X_1, X_2, X_3)$ una forma ternària sabem que aquesta no representa $\alpha \in \mathbb{Q}^*$ si i només si $\phi(X_1, X_2, X_3) - \alpha Y^2$ és no isotròpica si i només si $\delta(\phi - \alpha Y^2) = -\alpha\delta(\phi)$ és un quadrat. Per tant, ϕ com a màxim no representarà la classe de la inversa de $-\delta(\phi)$ mòdul quadrat. □

   Un cop vist aquesta proposició podem demostrar el cas de dimensió $n \geq 5$. N'hi ha prou amb suposar $n = 5$. Si mirem ϕ com $\phi = \omega_1(X_1, X_2, X_3) - \omega_2(Y_1, Y_2)$ suma de una forma ternària i una binària. Sabem que ω_1 representa totes les classes mòdul quadrat menys com a màxim una. Per la seva banda, la forma binària ω_2 representa com a mínim 2 classes mòdul quadrat. Per tant, hi ha almenys una classe mòdul quadrat representada per les dues formes, i això significa que tenen un element representat per les dues formes. Així doncs, ϕ és isotròpica.

   □

Acabat de demostrar el teorema 6.2 i recordant que ϕ representa a si i només si $\phi - aY^2$ és isotròpica podem establir la següent proposició.

Proposició 6.8. *Sigui $\alpha \in \mathbb{Q}_p^*$. La forma quadràtica ϕ de dimensió n, determinant $\delta \in \text{ıı}_p^*/(\mathbb{Q}_p^*)^2$, i invariant c representa α si i només si els seus invariants satisfan una de les següents condicions:*

1. $n = 1$ *i* $\alpha = \delta$.
2. $n = 2$ *i* $(\alpha, -\delta)_p = c$.
3. $n = 3$ *i* $\alpha \neq -\delta$.
4. $n = 3$ *i* $\alpha = -\delta$ *i* $(-1, -\delta)_p = c$.
5. $n \geq 4$.

Demostració. Com hem avisat abans totes són una aplicació bàsica del teorema 6.2 i la proposició 4.29.

En el primer cas, si $\dim \phi = 1$, llavors ϕ representa α si i només si el determinant de $\phi - \alpha Y^2$ que és $-\alpha\delta(\phi)$ és igual a -1. Això succeeix si i només si $\delta(\phi) = \alpha$.

En el segon cas, si $\dim \phi = 2$, llavors $\phi - \alpha Y^2$ és isotròpica si i només si $c(\phi - \alpha Y^2) = (-1, -\delta(\phi - \alpha Y^2))_p$. Si seguim el lema anterior això serà quan:

$$\begin{aligned} c(\phi) \cdot (\delta(\phi), -\alpha)_p = (-1, \alpha\delta(\phi))_p &\Leftrightarrow c(\phi) = (\delta(\phi), -\alpha)_p \cdot (-1, \alpha\delta(\phi))_p \\ &\Leftrightarrow c(\phi) = (\delta(\phi), -\alpha)_p \cdot (-1, \delta(\phi))_p \cdot (-1, \alpha)_p \\ &\Leftrightarrow c(\phi) = (\delta(\phi), \alpha)_p \cdot (-1, \alpha)_p = (-\delta(\phi), \alpha)_p. \end{aligned}$$

En el tercer cas, $\dim \phi = 3$, tenim que $\phi - \alpha Y^2$ no és isotròpica si i només si $c(\phi) \cdot (\delta(\phi), -\alpha)_p = (-1,-1)_p$ i $-\alpha\delta(\phi)$ és un quadrat. Això és equivalent a $\alpha = -\delta(\phi)$ i

$$\begin{aligned} & c(\phi) = (-1,-1)_p \cdot (\delta(\phi), -\alpha)_p \\ \Leftrightarrow\ & c(\phi) = (-1,-1)_p \cdot (\delta(\phi), \alpha^2\delta(\phi))_p = (-1,-1)_p \cdot (\delta(\phi), \delta(\phi))_p \\ \Leftrightarrow\ & c(\phi) = (-1,-1)_p \cdot (-\delta(\phi), \delta(\phi))_p \cdot (-1, \delta(\phi))_p = (-1, -\delta(\phi))_p. \end{aligned}$$

En el quart cas, on $\dim \phi \geq 4$, sabem que $\phi - \alpha Y^2$ serà sempre isotròpica al ser de dimensió més gran o igual que 5. □

Per últim, no voldríem acabar sense veure que els tres invariants determinant la forma quadràtica llevat d'equivalències.

Teorema 6.9. *Dos formes quadràtiques ψ, ω en Q_p són equivalents si i només si tenen la mateixa dimensió, el mateix determinant (en $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$) i el mateix invariant de Hasse.*

Demostració. Gràcies al teorema anterior, fent inducció en la dimensió, sabem que formes equivalents tenen els mateixos invariants. Ara volem veure la inversa, però per veure-la abans anunciarem una proposició:

Proposició 6.10. *Si tenim una forma quadràtica ϕ que representa α llavors aquesta es pot expressar com $\phi = \phi' + \alpha Y^2$, on ϕ' és una forma quadràtica de dimensió* $\dim \phi - 1$.

Demostració. Si ϕ representa α llavors sabem que tenim un element $x = (x_1, ..., x_m)$ tal que $\phi(x) = \alpha$. Sabem també per la proposició 4.17 que podem construir una base ortonormal on x n'és un vector. Veiem doncs que es compleix la proposició. □

Ara ja podem demostrar el teorema fent inducció des de n. Si ϕ i ω tenen els mateixos invariants hem vist que existirà un α que serà representat pels dos. Donat que com hem vist en la proposició 6.8 el fet que un element sigui representat o no per una forma quadràtica depèn exclusivament dels seus invariants.

També hem vist que si ϕ i ω representen α llavors ambdós poden ser expressats com $\phi = \phi' + \alpha Y^2$ i $\omega = \omega' + \alpha$, on ϕ' i ω' són formes quadràtiques de dimensió $n-1$ que tenen els mateixos invariants. Si iterem el procés per ϕ' i ω' arribaríem a veure que mateixos invariants impliquen mateixa forma quadràtica llevat de equivalència. □

7 Teorema de Hasse-Minkowski

Hem vist tot el necessari per demostrar el teorema de Hasse-Minkowski sobre formes quadràtiques en $\mathbb{Q}_p$. Recordem que el que anuncia és que una forma quadràtica en $\mathbb{Q}$ té solució no trivial si i només si la forma té solució no trivial en totes les seves completacions ($\mathbb{Q}_p$ i $\mathbb{R}$). Existeix un teorema més general que ens demostra que aquesta propietat no només la compleix el cos $\mathbb{Q}$ sinó qualsevol cos, una forma quadràtica té solució no trivial en un cos si en tenen totes les seves completacions. La demostració del cas general no la veurem aquí, però si que veurem la del cas particular de $\mathbb{Q}$.

Abans de començar el teorema, però, introduïm un teorema important que ens servirà a la demostració. En la demostració d'aquest teorema farem servir el teorema de Drichlet per progressions aritmètiques, anunciem-lo també.

Teorema 7.1. *Teorema de Drichlet per progressions aritmètiques. Per tota progressió aritmètica $a + b\lambda$, on $a, b \in \mathbb{Z}_{>0}$ són coprimers tenim infinits enters tals que $p = a + b\lambda$, on λ pren valors enters.*

La demostració d'aquest teorema no és gens senzilla i no la veurem en aquest treball. Personalment la demostració la tinc interioritzada després d'haver-la vist a l'assignatura de mètodes analítics en teoria de nombres a la UB. Consisteix en veure que la suma $\sum_{p \equiv a(b)} 1/p$ és divergent, i això s'aconsegueix mitjançant eines de la teoria analítica en teoria de nombres i aritmètica modular, concretament els caràcters Drichlet i el producte d'Euler. Però és tant extensa que no la veurem aquí.

Teorema 7.2. *Sigui $\{a_i\}$ un conjunt finit d'elements de $\mathbb{Q}^*$ i sigui $\{\epsilon_{i,p}\}$ un conjunt d'elements pertanyent a $\{-1, 1\}$ i on p significa tots els primers i ∞. Llavors existeix un element $x \in \mathbb{Q}^*$ que compleix que $(a_i, x)_p = \epsilon_{i,p}$ si i només si es compleixen les següents tres condicions:*

- *$\{\epsilon_{i,p}\}$ és 1 excepte per un nombre finit de casos.*
- *$\prod_p \epsilon_{i,p} = 1$.*
- *Per a tot p inclòs ∞, existeix x_p tal que $(a_i, x_p)_p = \epsilon_{i,p}$ per a tot i ó p.*

Observació 7.3. És important entendre el concepte del teorema, ja que un error conceptual podria fer pensar que aquest demostra el teorema de Hasse-Minkowski i no és així.

Demostració. Les dues primeres condicions provenen de que si $\epsilon_{i,p} = (x, a_i)_p$ llavors aquest ha de complir les propietats del producte de Hilbert. La propietat 3 es fàcil de veure entenent que $x_p = x$. Ara volem veure la implicació contrària. Comencem per multiplicar el conjunt $\{a_i\}$ per quadrats fins que tots siguin enters i a partir d'aquí definim dos conjunts:

- $P = \{p | p \text{ primer}\} \cup \{\infty\}$.
- Definim per $R = \{p \text{ primer } | p | a_1 a_2 \cdots a_s\} \cup \{2\} \cup \{\infty\}$, el conjunt finit de tots els factors primers de tots els $\{a_i\}$ amb l'afegit de 2 i ∞.
- Definim per T el conjunt finit de $p \in P$ tal que existeix almenys un $\epsilon_{i,p} = -1$.

Suposem que $R \cap T = \emptyset$, llavors si

$$a = \prod_{k \in T, k \neq 2, \infty} k, \quad m = 8 \prod_{k \in R, k \neq 2, \infty} k.$$

Com que $R \cap T = \emptyset$, els nombres a i m són coprimers. Només amb això ja podem aplicar el teorema de Drichlet de progressions aritmètiques i sabem que hi haurà un q primer tal que $q \notin R \cup T$ i $q \equiv a \pmod{m}$. Ara volem demostrar que $x = aq$ és el nombre racional que buscàvem. Aleshores volem veure que aquest nombre x és solució en totes les completacions de $\mathbb{Q}$.

- El primer cas és quan $p \in R$. Com que $R \cap T = \emptyset$, llavors sabem que $\epsilon_{i,p} = (a_i, x)_p = 1$ per a tot i. Com que x és positiu llavors $(a_i, x)_\infty = 1$ sempre. Ara veiem que

si $p = 2$ tenim que $x \equiv a^2 \pmod 8$ o si $p \neq 2$ llavors tenim que $x \equiv a^2 \pmod p$. Per tant, en qualsevol cas, a és una unitat p-àdica ja que p no divideix a. Per una aplicació senzilla del lema de Hensel sabem que x és un quadrat en $\mathbb{Q}_p$ per tant $\epsilon_{i,p} = (a_i, \gamma^2) = (a_i, 1) = 1$.

- El segon cas és quan $p \notin R$. En aquest cas a_i és una unitat p-àdica. Com hem vist en (5.5), si a_i és unitat p-àdica, llavors,

$$(a_i, \gamma)_p = (\frac{a_i}{p})^{ord_p(\gamma)}.$$

Per a tot γ pertanyent a $\mathbb{Q}_p^*$.
Si $p \notin T \cup \{p\}$, llavors x és una unitat p-àdica i per tant $(a_i, x)_p = 1$ per a tot a_i, el qual és el que buscàvem ja que $p \notin T$.
Si $p \in T$, llavors $ord_p(x) = 1$. Per la condició 3 sabem que tenim una solució p-àdica x_p tal que $(a_i, x_p) = \epsilon_{i,p}$. Com que $\epsilon_{i,p}$ és -1 per alguna i al ser $p \in T$, llavors tenim que $ord_p(x_p) \equiv 1 \pmod 2$, ja que del contrari tots els símbols de Hilbert serien 1. Per tant, aplicant la identitat anterior,

$$(a_i, x)_p = (\frac{a_i}{p})^{ord_p(x)} = (\frac{a_i}{p})^{ord_p(x_p)} = (a_i, x_p)_p = \epsilon_{i,j}.$$

Per últim, si $p = q$, llavors per el producte de Hilbert que compleix (a_i, x) i per la propietat 1 i 2 podem afirmar que:

$$(a_i, x)_q = \prod_{p \neq q} (a_i, x)_q = \prod_{p \neq q} \epsilon_{i,p} = \epsilon_{i,q}.$$

Per a tota i.

Per acabar, només queda veure que la suposició inicial de $R \cap T = \emptyset$ és innecessària. Per el teorema xinès del residu podem trobar un $x' \in \mathbb{Q}^*$ tal que $x'/x_p \in (\mathbb{Q}_p^*)^2$ per a tot $p \in R$ (podem exigir $x' \equiv x_p \pmod{p\mathbb{Z}_p}$ per a $p \neq 2$ i $x' \equiv x_2 \pmod{8\mathbb{Z}_2}$ per a $p = 2$ i $x/x_\infty > 0$), al ser R finit. Per tant, $(a_i, x')_p = (a_i, x_p)_p = \epsilon_{i,p}$ per a tot $p \in R$.

Ara definim $\mu_{i,p} = (a_i, x')_p \cdot \epsilon_{i,p}$. Clarament, μ compleix les condicions 1, 2 i 3 ja que $(a_i, x'x_p)_p = (a_i, x')_p \cdot \epsilon_{i,p} = \mu_{i,p}$. Per definició $\mu_{i,p} = 1$ quan $p \in R$, per tant, si redefiníssim els conjunts R i T adaptats a μ tindríem que son disjunts, i, aplicant el cas anterior, veuríem que existeix un $y \in \mathbb{Q}^*$ tal que $(a_i, y)_p = \mu_{i,p}$ per tot i, p. Per tant finalment, $x = yx'$ és la solució que buscàvem, ja que:

$$(a_i, yx')_p = (a_i, y)_p \cdot (a_i, x')_p = \mu_{i,j} \cdot (a_i, x')_p = (a_i, x')_p \epsilon_{i,p} \cdot (a_i, x')_p = \epsilon_{i,p}.$$

□

Sobre el teorema, tot i que pot semblar lògic que si totes les completacions tenen solució no trivial el cos original també, és un fet aïllat. Només succeeix generalment en formes quadràtiques.

Teorema 7.4. *Una forma quadràtica en $\mathbb{Q}$ és isotròpica si i només si ho és en totes les seves completacions $\mathbb{Q}_p$ i $\mathbb{R}$.*

La demostració es divideix en quatre casos segons la dimensió: quan és ≤ 2, quan és 3, quan és 4 i quan és major o igual que 5.

Primer cas: $n \leq 2$**.**
Per $n = 1$ passa que la forma quadràtica és ax^2 que té solució no trivial si i només si $a = 0$ en tots les completacions $\mathbb{Q}_p$ i $\mathbb{R}$. Coincideix amb els casos que té solució no trivial en $\mathbb{Q}$, que és només quan $a = 0$.

Per $n = 2$ necessitarem el següent lema.

Lema 7.5. *Una forma quadràtica binària $ax^2 + bxy + cy^2$ és isotròpica si i només si el discriminant $b^2 - 4ac$ és un quadrat en $\mathbb{Q}_p$.*

Demostració. Veiem la identitat

$$(2ax - by)^2 - y^2(b^2 - 4ac) = 4a(ax^2 + bxy + cy^2).$$

A partir de la identitat és fàcil veure que si la forma és isotròpica el discriminant ha de ser un quadrat. En tant que si la solució no trivial té $y \neq 0$ llavors

$$b^2 - 4ac = \frac{(2ax - by)^2}{y^2}.$$

Al ser divisió de quadrats el discriminant és un quadrat. Si $y = 0$, llavors $2ax = 0$. La variable x no pot ser 0 perquè llavors la solució seria trivial. Per tant, $a = 0$, i finalment $b^2 - 4ac = b^2$ i per tant és un quadrat.

La implicació contrària és senzilla, ja que si el discriminant és un quadrat, posem que $b^2 - 4ac = \gamma^2$ llavors,

$$(2ax - by)^2 - y^2(b^2 - 4ac) = (2ax - by - yu) \cdot (2ax - by + yu)$$

Per tant $(x, y) = (b - u, 2a)$ és solució no trivial. □

Demostració. Havent vist aquest lema ja podem demostrar el teorema de Hasse-Minkowski per formes binàries. Sabem que en $\mathbb{R}$ la forma $ax^2 + bxy + cy^2$ és isotròpica si i només si el discriminant no és negatiu. Ara, per mirar els casos en el que el cos és $\mathbb{Q}_p$, escrivim el discriminant $D = b^2 - 4ac$ en descomposició de nombrés primers.

$$D = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Per a que la forma quadràtica tingui solució en $\mathbb{Q}_{p_i}$ la condició de que el discriminant sigui un quadrat en $\mathbb{Q}_{p_i}$ és equivalent a que el ordre p_i-àdic de D sigui parell, $ord_{p_i}(D) \equiv 0 \pmod 2$. És a dir, que α_i sigui parell per a tot primer de la seva descomposició. És a dir, que D sigui un quadrat en $\mathbb{Q}$.

Per altra banda, tenim que $ax^2 + bxy + cy^2$ té solució no trivial en $\mathbb{Q}$ si i només si el discriminant és un quadrat positiu. Per tant, veiem que les condicions per a que tingui solució no trivial a $\mathbb{Q}$ són les mateixes per a que tingui solució no trivial en totes les completacions $\mathbb{Q}_p$ i $\mathbb{R}$. Queda demostrat el teorema per dimensions menors o iguals a 2.□

Segon cas: $n = 3$**.**

Demostració. La demostració per aquest cas necessita concentració perquè s'utilitzen raonaments nous en aquest tema. L'estudi d'aquest cas s'atribueix a Legendre.
Tenim una forma quadràtica ternària ϕ i per conveniència l'expresem en forma diagonal $a'x^2 + b'y^2 + c'z^2$. Si tenim un coeficient igual a 0 llavors clarament tenim un zero no trivial en $\mathbb{Q}$, $\mathbb{Q}_p$ i $\mathbb{R}$. Per tant, a partir d'ara suposem que cap coeficient és zero. Multiplicant ϕ per racionals adients podem aconseguir que els tres coeficients pertanyin a $\mathbb{Z}$. Finalment, si arribats a aquest punt el primer coeficient és α, podem multiplicar ϕ per α i fer un canvi de variable de x per x/α i finalment, la nostra forma ternària tindria la forma $x^2 - ay^2 - bz^2$ per $a, b \in \mathbb{Z}$ enters lliures de quadrats (ja que si p^2 divideix algun coeficient el podem simplificar amb un canvi de variable).

Per demostrar el teorema de Hasse-Minkowski per formes ternàries farem una inducció en $m = |a| + |b|$. El cas inicial és $m = 2$. Per $m = 2$ les formes són del tipus $x^2 \pm y^2 \pm z^2$. Només la forma amb tots els coeficients positius no és isotròpica en totes les completacions, ja que no ho és per $\mathbb{R}$. I tampoc ho és en $\mathbb{Q}$. La resta tenen solucions no trivial senzilles del tipus $(x, y, z) = (0, 1, 1)$ ó $(1, 0, 1)$ ó $(1, 1, 0)$ en funció de la forma.

La dificultat ve quan suposem $m > 2$. Suposem que $|b| > |a|$. Suposem que tenim solucions no trivials per a totes les completacions $\mathbb{Q}_p$ i $\mathbb{R}$ i volem veure que llavors $\mathbb{Q}$ també té una solució, de moment en el cas $m = 2$ és el que ha passat. Llavors succeeix que $x^2 = ay^2 + bz^2$. Sabent això volem veure que a és un quadrat mòdul b. Per veure-ho, descomponem b en producte de primers. Al ser lliure de quadrats no n'hi ha cap amb potència major que 1, per tant $b = p_1 \cdots p_r$. Demostrarem que a és un quadrat mòdul p_i per tots els divisors p_i de b.

Per demostrar-ho, veiem que tenim una solució $x^2 = ay^2 + bz^2$ en $\mathbb{Q}_{p_i}$ i podem assumir que de x, y, z almenys un és una unitat. Veiem ara doncs,

$$x^2 = ay^2 + bz^2 \equiv ay^2 \pmod{p_i\mathbb{Z}_{p_i}}.$$

Si $p_i|a$ llavors ja estem. Per tant, suposarem que a és una unitat p_i-àdica. Tenim que $y \neq 0$ perquè llavors b seria un quadrat i tenim que y ha de ser una unitat. Donat que de no ser-ho llavors per complir que $ord_{p_i}(x^2) = ord_{p_i}(ay^2 + bz^2)$ tindríem que $ord_{p_i}(x) \geq 1$ i per conseqüent, i per propietats de l'ordre p-àdic, $ord_{p_i}(bz^2)$ hauria de ser major o igual que 2 i per tant $ord_{p_i}(z) \geq 1$. Això contradiu que almenys una coordenada de la solució és una unitat en $\mathbb{Z}_{p_i}$.

Per tant, al ser y unitat podem definir correctament $a \equiv x^2/y^2 \equiv (x/y)^2 \pmod{p_i\mathbb{Z}_{p_i}}$, on a és un quadrat en $\mathbb{Z}/p_i\mathbb{Z}$ per cada divisor p_i de b. Aleshores ho és mòdul b. El que significa que existeix γ tal que $\gamma^2 = a + bb'$. A més, podem escollir $\gamma \leq |b|/2$. Si reordenem l'equació ens trobem que $bb' = \gamma^2 - a$ té el valor d'una norma en l'extensió algebraica $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$ o $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ segons convingui. Per la proposició (5.2) sabem que llavors, al ser bb' norma de l'extensió, tenim:

$$(a, bb')_p = (a, b)_p \cdot (a, b')_p = 1.$$

D'una manera semblant a la demostració de (5.2) sabem que $x^2 - ay^2 - by^2$ serà isotròpica si i només si $x^2 - ay^2 - b'z^2$ ho és en K, tant per $\mathbb{Q}$ com per $\mathbb{Q}_p$ i $\mathbb{R}$. Com que hem assumit

que la primera tenia solució la segona també.
Ara només queda veure que $|b'| < |b|$ i és que al ser $b \geq 2$:

$$|b'| = |\frac{\gamma^2 - a}{b}| \leq |\frac{b}{4}| + 1 < |b|$$

Per tant, la nova forma $\phi'' = x^2 - ay^2 - b''z^2$, on b'' és b' després d'haver simplificat els factors quadrats, tindrà $m' = |a| + |b''|$ menor que m. Per tant, podem iterar el procés fins arribar a un cas inicial, i mantenint la condició que si té solució no trivial en totes les completacions llavors la té en $\mathbb{Q}$.

□

Ja hem acabat doncs la demostració per el cas $n = 3$. Hem suposat que totes les completacions tenien solució i hem trobat que el cos dels racionals $\mathbb{Q}$ també té una solució. Ara demostrarem el cas $n = 4$, però abans necessitem una proposició que ens ajudarà en la demostració.

Proposició 7.6. *Si sabem que una forma quadràtica ternària ϕ és isotròpica en totes les completacions $\mathbb{Q}_p$ i $\mathbb{R}$ menys com a màxim una que desconeixem, immediatament sabem que aquesta serà isotròpica també.*

Demostració. Si no és regular sempre serà isotròpica. Si ho és, representem ϕ en forma diagonal $\alpha X_1^2 + \beta X_2^2 + \gamma X_3^2$. Per el teorema (6.2) sabem que ϕ és isotròpica si i només si

$$(-1, -\alpha\beta\gamma)_p = c(\phi) = (\alpha, \beta)_p \cdot (\alpha, \gamma)_p \cdot (\beta, \gamma)_p$$

Com que cada símbol de Hilbert per individual compleix el producte de Hilbert, llavors sabent que la equació és certa per a totes les completacions menys una veiem que aquesta també ha de complir l'equació. □

Tercer cas: $n = 4$**.**

Demostració. En aquest cas escrivim ϕ en forma diagonal $a_1x_1^2 + a_2x_2^2 - a_3x_3^2 - a_4x_4^2$, i la visualitzem com dues formes quadràtiques binàries: $\omega_1 = a_1x_1^2 + a_2x_2^2$ per una banda i $\omega_2 = a_3x_3^2 + a_4x_4^2$ per l'altra, per tant $\phi = \omega_1 - \omega_2$. Fem la nostra suposició habitual que diu que tenim solució no trivial en totes les completacions. Llavors tenim que si ϕ és isotròpica llavors existeix un $\alpha \in \mathbb{Q}_p^*$ representat per les dues funcions binàries ω_1 i ω_2. Per la proposició (6.4) sabem que per un element $\beta \in \mathbb{Q}_p$ qualsevol:

$$\beta \text{ està representat per } \omega_1 \Leftrightarrow (\beta, -a_1a_2)_p = (a_1, a_2)_p$$
$$\beta \text{ està representat per } \omega_2 \Leftrightarrow (\beta, -a_3a_4)_p = (a_3, a_4)_p$$

Com que hem suposat que hi ha solucions per totes les completacions sabem que per a cada completació existeix un β_p representat per les dues formes. Podem aplicar llavors el teorema (7.2) amb $\{a_i\} = \{-\alpha_1\alpha_2\}$ i $\epsilon_{i,p} = (\alpha_1, \alpha_2)_p$, tenim que existeix $c \in \mathbb{Q}^*$ tal que

$$(c, -\alpha_1\alpha_2)_p = (\alpha_1, \alpha_2)_p \text{ i } (c, -\alpha_3\alpha_4)_p = (\alpha_3, \alpha_4)_p,$$

per tota completació $\mathbb{Q}_l$ ó $\mathbb{R}$. Per tant, $\alpha_1y_1^2 + \alpha_2y_2^2 - cy_3^2$ és isotròpica en totes les completacions, i per la demostració del teorema Hasse-Minkowski per $n = 3$, també ho és en $\mathbb{Q}$. Per tant $\alpha_1y_1^2 + \alpha_2y_2^2$ representa c en $\mathbb{Q}$. Anàlogament, sabem que $\alpha_3y_3^2 + \alpha_4y_4^2$ representa també c en $\mathbb{Q}$ i per tant $\phi = \alpha_1y_1^2 + \alpha_2y_2^2 - \alpha_3y_3^2 - \alpha_4y_4^2$ és isotròpica en $\mathbb{Q}$. □

Quart i últim cas: $n \geq 5$**.**

Demostració. Comencem suposant que $n = 5$ i que tenim ϕ en forma diagonal $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2$ tal que $a_1 > 0$ i $a_5 < 0$ (ja que si tots els coeficients tenen el mateix signe llavors no té solució no trivial en $\mathbb{R}$). Llavors definim $P = \{p \in \mathbb{Z} | p \text{ primer } \} \cup \{\infty\}$ i $\omega_1 = a_1x_1^2 + a_2x_2^2$ i $\omega_2 = -a_3x_3^2 - a_4x_4^2 - a_5x_5^2$. Ara, com que tenim que $\omega_1 - \omega_2 = \phi$ és isotròpica en $\mathbb{Q}_p$ llavors per cada $p \in P$ existeix un α_p representat per ω_1 i ω_2. Anàlogament al cas anterior, sabem que existeix un $\alpha \in \mathbb{Q}^*$ tal que ω_1 representa α en totes les completacions. De la manera en com hem construït aquest α sabem que també el genera ω_2. Per tant, anàlogament al cas anterior també sabem que ω_1 i ω_2 generen α en $\mathbb{Q}$ de manera que ja està demostrat.

Finalment, si tenim $n \geq 5$ i tenim que no tots els coeficients són del mateix signe (equivalent a tenir solució en $\mathbb{R}$). Llavors té solució en $\mathbb{Q}$ ja que podem expressar $\phi = \phi_1 + \phi_2$ on ϕ_1 té dimensió 5 i els dos coeficients amb signes oposats. Per tant ϕ_1 és isotròpica en $\mathbb{Q}$ i aleshores ϕ també. □

8 Aplicacions

Però és realment útil aquest teorema? Com tot en les matemàtiques el concepte útil és relatiu, a més, res no és inútil fins que es demostri el contrari, ja que les aplicacions poden estar per descobrir.

En aquest cas aquest problema té bastantes aplicacions com les que veurem seguidament. Per començar és un teorema que va diferenciar quan les formes quadràtiques tenen solucions en els racionals i quan no, per tant l'aportació en el camp de la teoria de nombres és important, Gauss i Legendre també van complementar la teoria per saber quines són aquestes solucions i com trobar-les.

Una aplicació que veurem seguidament és com un nombre enter per un seguit de condicions serà la suma de tres o menys quadrats enters. Necessitarem d'unes proposicions prèvies.

Proposició 8.1. *Una forma quadràtica regular amb coeficients racionals representa $c \in \mathbb{Q}^*$ en $\mathbb{Q}$ si i només si c és representada en $\mathbb{R}$ i tots els cossos p-àdics $\mathbb{Q}_p$.*

Demostració. És obvi aplicant el teorema de Hasse-Minkowski i la proposició 4.29.
La forma ϕ representa c en $\mathbb{Q}$ si i només si $\phi - cY^2$ és isotròpica en $\mathbb{Q}$ si i només si és isotròpica en en $\mathbb{Q}_p$ i en $\mathbb{R}$ si i només si ϕ representa c en totes les completacions. □

Per tant podem saber completament quan una forma quadràtica representa un element racional c en $\mathbb{Q}$. Com també tenim completament diferenciat quan una forma quadràtica ϕ és isotròpica en $\mathbb{Q}$.

Proposició 8.2. *Sigui ϕ una forma quadràtica regular de dimensió n amb coeficients en $\mathbb{Q}$ i amb determinant $\delta(\phi) \in \mathbb{Q}/\mathbb{Q}^2$, llavors ϕ representa c si i només si succeeix algun fet dels següents:*

- $n = 2$ *i* $\delta(\phi) = -1$ *en* $\mathbb{Q}/\mathbb{Q}^2$.
- $n = 3$ *o* $n = 4$ *i* ϕ *és isotròpica en* $\mathbb{R}$ *i en* $\mathbb{Q}_2$ *i* $\mathbb{Q}_p$ *per tots els* p *per als que* $ord_p(\delta(\phi))$ *sigui imparell.*
- $n \geq 5$ *i* ϕ *isotròpica en* $\mathbb{R}$.

Demostració. La demostració per els casos $n = 2$ ó $n \geq 5$ l'hem vist anteriorment. Per els casos $n = 3, 4$ suposem $n = 3$ i veiem que si l'ordre p-àdic del determinant és imparell, o bé tots tres coeficients tenen ordre senar o bé almenys dos el tenen parell. En el primer cas és isotròpica ja que q/p té dimensió 3 i els tres coeficients són unitats. En el segon cas, els dos coeficients a i b compleixen $(a, b)_p = 1$ i com vam veure $(-1, -\delta)_p = \epsilon = (a, b)_p = 1$, per tant és isotròpica en ambdós casos. □

Ara ja tenim la informació per saber quan una forma quadràtica representa c en $\mathbb{Q}$.

Proposició 8.3. *Una forma quadràtica regular* ϕ *de dimensió* n *representa* c *en* $\mathbb{Q}$ *si i només si es compleix alguna de les següents condicions:*

- $n = 1$ *i* $c/\delta(\phi)$ *és un quadrat en* $\mathbb{Q}$.
- $n = 2$ *ó* $n = 3$ *i* ϕ *isotròpica en* $\mathbb{R}$, $\mathbb{Q}_2$ *i en* $\mathbb{Q}_p$ *en els primers tal que* $ord_p(\delta(\phi)) \not\equiv 0 \pmod 2$.
- $n \geq 4$ *i* ϕ *és isotròpica en* $\mathbb{R}$.

La demostració és òbvia, fruit de la proposició d'abans.

Per les següents proposicions i per arribar al teorema de Davenport-Cassels sobre enters expressats en quadrats necessitem les següents definicions. Recordem que com vam explicar en el tema de formes quadràtiques, una forma quadràtica $\phi(x_1, ..., x_n)$ pot ser vista com un producte de vectors i matrius de la forma $V^T MV$, on $V = (x_1, ..., x_n)$ i M una matriu quadrada.

Definició 8.4. *Direm que una forma quadràtica* ϕ *pren valors enters o directament que és entera quan per qualsevol* $x \in \mathbb{Z}^k$ *tenim que* $\phi(x) \in \mathbb{Z}$.

És fàcil veure que això succeeix quan tots els coeficients de la diagonal de la matriu representativa són enters i els de fora de la diagonal són enters o múltiples de $\frac{1}{2}$.

Definició 8.5. *Direm que* ϕ *té matriu entera quan la forma bilineal definida per* $\psi(x, y) = \frac{1}{4}(\phi(x + y) - \phi(x - y))$ *és entera per qualsevol* $x, y \in \mathbb{Z}^k$.

Això és equivalent a dir que tots els coeficients de la matriu representativa són enters.

Proposició 8.6. *Sigui* ϕ *una forma quadràtica definida positiva amb matriu entera de dimensió* k *tal que per a tot* $x \in \mathbb{Q}^k$ *existeix* $y \in \mathbb{Z}^k$ *tal que* $\phi(x - y) < 1$, *llavors* ϕ *representa* $n \in \mathbb{Z}$ *en* $\mathbb{Z}$ *si i només si ho fa en* $\mathbb{Q}$.

Demostració. Per hipòtesi tenim que per alguna fracció $a/b \in \mathbb{Q}$ tenim que $\phi(a/b) = n$ on $a, b \in \mathbb{Z}$, o el que és el mateix, existeix un enter a tal que $\phi(a) = n \cdot b^2$. Triem a de manera que b^2 és el més petit possible, i veiem ara que $b = 1$.

Per hipòtesi sabem que existeix un $y \in \mathbb{Z}^k$ tal que $a/b = y + z$, on $\phi(z) < 1$. Com que ϕ és definida positiva, tenim dos casos:
Si $\phi(z) = 0$ llavors és immediat ja que $a/b = y \in \mathbb{Z}^k$ i com que b és mínima tenim que $b = 1$.
Si $\phi(z) > 0$ llavors definim quatre valors:

$$c = \phi(y) - n,\ d = 2(bn - \psi(a, y)),\ b' = cb + d,\ a' = ca + dy.$$

Al tenir ϕ matriu entera llavors tenim que $c, d, b' \in \mathbb{Z}$ i $a' \in \mathbb{Z}^k$, i a més:

$$\begin{aligned}\phi(a') &= \psi(ca + dy, ca + dy) = c^2\psi(a, a) + 2cd\psi(a, y) + d^2\psi(y, y)\\ &= c^2b^2n + cd(2nb - d) + d^2(c + n) = n(c^2b^2 + 2cdb + d^2) = n(cb + d)^2 = nb'^2.\end{aligned}$$

Hem trobat un nou quadrat múltiple de n representat per ϕ en $\mathbb{Z}$, que a més, al comparar-los, veiem que $d' < d$. Som-hi:

$$\begin{aligned}bb' &= cb^2 + db = b^2\psi(y, y)b^2n + +2b^2n2b\psi(a, y) = b^2\psi(y, y)2b\psi(a, y) + \psi(a, a)\\ &= \psi(by - a, by - a) = \psi(z, z)b^2.\end{aligned}$$

Com hem vist abans, teníem que $\psi(z, z) < 1$ per tant, tenim que $bb' < b^2 \Rightarrow b' < b$. I aquest fet és contradictori amb que escollíssim b minimal, per tant $b = 1$ per reducció a l'absurd. □

Definició 8.7. *Una forma quadràtica que té matriu entera de dimensió k és fortament euclidiana si per a tot $x \in \mathbb{Q}^k$ existeix $y \in \mathbb{Z}^k$ tal que $\phi(x - y) < 1$.*

Coincideix amb les matrius que compleixen les condicions de la proposició anterior, i de fet no ho veurem però hi ha un nombre finit de formes quadràtiques que ho compleixen. No veurem quines però l'important és saber que

$$\phi_1 = x_1^2,\ \phi_2 = x_1^2 + x_2^2 \text{ i } \phi_3 = x_1^2 + x_2^2 + x_3^2$$

ho són.

Definició 8.8. *Una forma quadràtica que té matriu entera de dimensió k és euclidiana si per a tot $x \in \mathbb{Q}^k$ existeix $y \in \mathbb{Z}^k$ tal que $\phi(x - y) \leq 1$.*

Observació 8.9. Totes les formes fortament euclidianes són euclidianes.

Hi ha exemples de formes quadràtiques euclidianes que representen elements en $\mathbb{Q}$ i no en $\mathbb{Z}$. Però com veurem seguidament $x_1^2 + x_2^2 + x_3^2 + x_4^2$ és un cas de forma euclidiana, no fortament euclidiana que representa un enter n en $\mathbb{Q}$ si i només si el representa en $\mathbb{Z}$.

Proposició 8.10. *La forma quadràtica $\phi = x_1^2 + x_2^2 + x_3^2 + x_4^2$ representa un enter n en $\mathbb{Q}$ si i només si el representa en $\mathbb{Z}$.*

Demostració. Només hem de demostrar que si ho representa en $\mathbb{Q}$ llavors ho fa en $\mathbb{Z}$.
Primer veiem que $\phi(x_1, x_2, x_3, x_4)$ compleix la propietat anterior per tot $(x_1, x_2, x_3, x_4) \in \mathbb{Q}^4$ excepte si $(x_1, x_2, x_3, x_4) \in (\frac{1}{2} + \mathbb{Z})^4$ ja que per a tot x_i podem restar-li un enter y_i tal que $|x_i - y_i| \leq \frac{1}{2}$, essent la inequació estricta només en el cas que hem indicat abans, per tant, per a tota la resta

$$\phi(x_1 - y_1, ..., x_4 - y_4) < (1/2)^2 + (1/2)^2 + (1/2)^2 + (1/2)^2 = 1/4 \cdot 4 = 1.$$

Si tenim que $x/d = y + z$ i $\phi(z) < 1$ llavors podem aplicar la proposició 8.6, sinó, tenim el cas $\phi(z) = 1$ on ja hem vist que llavors $z \in (\frac{1}{2} + \mathbb{Z})^4$, per tant $x/\frac{d}{2} \in 1 + 2\mathbb{Z}$ i per tant podem dividir x (cada x_i) per $\frac{d}{2}$ i seria enter per tant contradiríem el fet que d és minimal per a tot $d \neq 2$. Suposem doncs que $d = 2$ i llavors veiem la següent identitat:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

$$z_1 = x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4,\ z_2 = x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3,$$
$$z_3 = x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2,\ z_4 = x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1.$$

Si canviem de signe cada x_i, al ser imparells podem aconseguir que tots els $x_i \equiv 1 \pmod 4$, a més podem definir $y = (1/4, -1/4, -1/4, -1/4)$ i seguint la identitat anterior tindrem uns coeficients z_i que seguint l'algorisme de construcció han de ser enters tal que $\phi(z) = \phi(x) \cdot \phi(y) = 4n \cdot 1/4 = n$. Demostrat. □

Teorema 8.11. *(Gauss). Sigui $a \in \mathbb{Q}^*$, serà suma de tres quadrats si i només si a és positiva i no és de la forma $4^\alpha(8b - 1)$, per $\alpha, b \in \mathbb{Z}$.*

Demostració. La completació dels reals implica que ha de ser positiva. Com hem vist en la proposició 6.8 l'únic cas en que no representa un element a és quan $a = -\delta$ és igual al determinant mòdul quadrat i $(-1, -\delta)_p = c$. En aquest cas la nostra forma quadràtica $(x_1^2 + x_2^2 + x_3^2)$ té $\delta = 1$ i $c = 1$ per tant $(-1, -1)_p$ és sempre 1 ja que són tres unitats excepte en $\mathbb{Q}_2$, on $(-1, -1)_2 = -1 \neq 1$, per tant hem d'evitar que $a = -\delta$ si volem que sigui representat per la suma de tres quadrats, això és equivalent a dir que $-a$ no sigui un quadrat i això és equivalent a dir que $a/2^{ord_2(a)} \not\equiv 7(8)$ que és equivalent a dir que a no és de la forma $a = 4^\alpha(8b - 1)$. □

Veiem que en 4 quadrats es poden cobrir tots els enters positius.

Teorema 8.12. *(Lagrange). Tot enter positiu és suma de 4 quadrats.*

Demostració. Sigui n un enter positiu, podem escriure aquest de manera única com $n = 4^\alpha m$, on m no és divisible per 4.
Si mirem m mòdul 8 obtenim que per $m \equiv 1, 2, 3, 5, 6 \pmod 8$ m pot ser expressat com a suma de tres quadrats $m = x_1^2 + x_2^2 + x_3^2$, $x_1, x_2, x_3 \in \mathbb{Z}$ i per tant $n = (2x_1)^2 + (2x_2)^2 + (2x_3)^2$ també.
Si $m \equiv 7 \pmod 8$ llavors $m - 1$ pot ser expressat com a suma de tres quadrats i n com $n = 4^\alpha(m-1) + 4^\alpha$, on el primer sumand és una suma de tres quadrats i el segon sumand és un quadrat, per tant en aquest cas n és suma de 4 quadrats. □

Exemple 8.13. Per ajudar a tenir una idea més concreta de l'abast d'aquest teorema escrivim com a suma de quadrats els primers 40 nombres.

$1 = 1^2$, $11 = 3^2 + 1^2 + 1^2$, $21 = 4^2 + 2^2 + 1^2$, $31 = 5^2 + 2^2 + 1^2 + 1^2$,
$2 = 1^2 + 1^2$, $12 = 2^2 + 2^2 + 2^2$, $22 = 3^2 + 3^2 + 2^2$, $32 = 4^2 + 4^2$,
$3 = 1^2 + 1^2 + 1^2$, $13 = 3^2 + 2^2$, $23 = 3^2 + 3^2 + 2^2 + 1^2$, $33 = 4^2 + 4^2 + 1^2$,
$4 = 2^2$, $14 = 3^2 + 2^2 + 1^2$, $24 = 4^2 + 2^2 + 2^2$, $34 = 5^2 + 3^2$,
$5 = 2^2 + 1^2$, $15 = 3^2 + 2^2 + 1^2 + 1^2$, $25 = 5^2$, $35 = 5^2 + 3^2 + 1^2$,
$6 = 2^2 + 1^2 + 1^2$, $16 = 4^2$, $26 = 5^2 + 1^2$, $36 = 6^2$,
$7 = 2^2 + 1^2 + 1^2 + 1^2$, $17 = 4^2 + 1^2$, $27 = 5^2 + 1^2 + 1^2$, $37 = 6^2 + 1^2$,
$8 = 2^2 + 2^2$, $18 = 3^2 + 3^2$, $28 = 5^2 + 1^2 + 1^2 + 1^2$, $38 = 6^2 + 1^2 + 1^2$,
$9 = 3^2$, $19 = 3^2 + 3^2 + 1^2$, $29 = 5^2 + 2^2$, $39 = 6^2 + 1^2 + 1^2 + 1^2$,
$10 = 3^2 + 1^2$, $20 = 4^2 + 2^2$, $30 = 5^2 + 2^2 + 1^2$, $40 = 6^2 + 2^2$.

Les representacions no són úniques, per exemple 27 també pot ser escrit com $3^2 + 3^2 + 3^2$ ó 28 com $4^2 + 2^2 + 2^2 + 2^2$.

De regal també obtenim un teorema sobre els nombres triangulars.

Teorema 8.14. *Tot nombre natural enter és suma de 3 nombres triangulars.*

Demostració. Recordem que un nombre triangular és aquell que té la forma $t = \frac{m(m+1)}{2}$, amb m enter. Llavors si volem representar com a suma de tres nombres triangulars un enter n apliquem el teorema anterior per al enter $8n + 3$, com que $8n + 3 \not\equiv 7 \pmod 8$ llavors tenim que és suma de tres quadrats.

$$x_1^2 + x_2^3 + x_3^2 = 8n + 3, \quad \Rightarrow \quad x_1^2 + x_2^3 + x_3^2 \equiv 3 \pmod 8,$$

Però en mòdul 8 només els residus 0,1 i 4 són quadrats per tant l'única possibilitat és que $x_1^2, x_2^2, x_3^2 \equiv 1 \pmod 8$ i, per tant, x_1, x_2, x_3 imparells, que és el que ens importa, ja que això significa que existeix un enter m_i tal que $x_i = 2m_i + 1$. Aquests enters m_i seran la clau de la solució ja que:

$$\sum_{i=1,2,3} \frac{m_i(m_i+1)}{2} = \frac{1}{8}((\sum_{i=1,2,3} (2m_i+1)^2) - 3) = \frac{1}{8}(8n + 3 - 3) = n.$$

□

Tenim una demostració que a més ens indica com obtenir els nombres triangulars a partir dels quadrats.

9 Contraexemples

El principi local-global consisteix en que una propietat es compleix globalment si i només si és compleix localment a tot arreu. Hem vist que aquest principi es compleix en les solucions racionals en formes quadràtiques de coeficients racionals. Potser l'eufòria i l'efervescència del moment ens pot fer pensar que podem ampliar aquest principi a tots els

polinomis i així tenir ben diferenciades les solucions per a tots els polinomis en $\mathbb{Q}$.

Sense voler ser un aixafa-guitarres en aquest tema veurem que en general no és així.

Comencem però en un cas en que si es compleix com són les equacions de segon grau amb una sola variable.

Proposició 9.1. *Una equació de segon grau en una sola variable compleix el principi local-global.*

Demostració. Com hem vist en el lema 7.5, veiem que $ax^2+bxy+cy^2$ té solució no trivial si i només si la té per a totes les completacions.
Per $a \neq 0$ tenim que per una solució (x', y'), la variable y' ha de ser diferent de 0 ja que de ser-ho tindríem que $ax'^2 = 0$ que implicaria $x' = 0$ i la solució passaria a ser trivial. Així doncs veiem que (x', y') és solució de $ax^2 + bxy + cy^2$ si i només si $\frac{x'}{y'}$ és solució de $f(z) = az^2 + bz + c$ per $a \neq 0$.
El raonament que hem fet és tant vàl·lid per $\mathbb{Q}$ com per les seves completacions, per tant la conclusió és que $f(x)$ té solució en $\mathbb{Q}$ si i només si la té en totes les seves completacions $\mathbb{Q}_p$ i $\mathbb{R}$. □

Proposició 9.2. *Les equacions*

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0,$$
$$(x^2 - 2)(y^2 - 17)(z^2 - 34) = 0.$$

tenen solucions en totes les completacions però no en tenen en $\mathbb{Q}$.

Demostració. La demostració és anàloga als dos casos, i és que tenen solució si i només si un dels productes té solució, és a dir, si alguna de les arrels $\sqrt{2}, \sqrt{17}, \sqrt{34}$ pertanyi al cos en el que estiguem.
Primer veiem que és obvi que no tindrà solució en $\mathbb{Q}$ ja que cap dels nombres són quadrats i en canvi si que en tindrà en $\mathbb{R}$.
Després veiem que en $\mathbb{Q}_2$ succeeix que 17 és un quadrat ja que $17 \equiv 1 \pmod 8$, com també tenim que 2 és un quadrat en $\mathbb{Q}_{17}$ ja que $(\frac{2}{17}) = 1$.
Finalment tenim que per a tots els primers $p \neq 2, 17$ tenim que $(\frac{2}{p})(\frac{17}{p})(\frac{34}{p}) = 1$ per tant algun ha de ser 1, i per tant algun ha de ser un quadrat. □

Ja tenim el primer contraexemple, aquest segurament el més fàcil de demostrar, i de grau 6. Ens agradaria veure algun contraexemple de grau 3 ja que acotaria bastant l'estudi dels contraexemples, i de fet n'hi ha. No ho veurem aquí ara però el matemàtic Ernst Selmer va descobrir que l'equació $3x^3 + 4y^3 + 5z^3 = 0$ té solucions en totes les completacions però no en $\mathbb{Q}$. Ens haurem de conformar amb el següent exemple de grau 4. En qualsevol cas, si algú volgués veure la demostració del contraexemple de Selmer pot trobar-la a [7].

Proposició 9.3. *L'equació*

$$y^2 + z^2 = (3 - x^2)(x^2 - 2),$$

no compleix el principi local-global.

Demostració. Aquesta demostració ja és més complexa.
Una solució en $\mathbb{R}$ seria $(x, y, z) = (\sqrt{2}, 0, 0)$. Per la resta de $\mathbb{Q}_p$, amb la demostració de 4.27 sabem que si assignem $x = 1$ tenim que la part dreta de l'equació equival a -2 i això és generat per dos quadrats en tots els $\mathbb{Q}_p$ per $p \neq 0$.
Per últim, en el cas $\mathbb{Q}_2$ tenim que si $x = 1$ llavors la part dreta equival a -6, la proposició 3.23 ens recorda que $\sqrt{-7}$ és un quadrat en $\mathbb{Q}_2$ i per tant que $(x, y, z) = (0, \sqrt{-7}, 1)$ és una solució.

Ara només quedaria veure que no té solució en $\mathbb{Q}$, que sol ser el més complicat. Comencem per suposar que hi ha una solució racional, i que per tant si multipliquem per el mínim comú dels divisors tenim que l'equació

$$a^2 + b^2 = (3D^2 - c^2)(c^2 - 2D^2)$$

té solució entera. De totes les solucions escollim la que té D minimal, el primer que volem veure és que el màxim comú divisor de c i D no pot ser dividit per 2 ni per primers $p \equiv 3 \pmod 4$. Suposant que fos cert, tindríem $a^2 + b^2 \equiv 0 \pmod{p^4}$, i per aquests p tenim que -1 no és un quadrat, per tant això implicaria $p|a, b, c, D$ que es contradiu amb el fet que D sigui minimal.
Finalment, un cop hem vist que per positivitat s'ha de complir que $2D^2 < c^2 < 3D^2$, considerem dos casos. El primer és que entre c i D un dels dos és imparell, llavors $3D^2 - c^2 \equiv 3 \pmod 4$, i per tant hi ha un divisor $p \equiv 3 \pmod 4$ que elevat a una potència imparella divideix $3D^2 - c^2$, i que al no dividir $c^2 - 2D^2$ ja que del contrari tindríem que $p|c, D$ per tant divideix $a^2 + b^2$ per la mateixa potència imparella, que és impossible ja que implicaria que $p^3|a^2, b^2$ però $p^4 \nmid a^2, b^2$ el qual no és possible.
El segon i últim cas és en el que D i c són imparells (no contemplem que els dos siguin parells perquè contradiria el que hem vist abans). Per aquest cas tenim que $c^2 - 2D^2 \equiv 3 \pmod 4$ i la resta de la demostració és anàloga. □

10 Conclusions

Les úniques normes en $\mathbb{Q}$ són l'euclidiana i la p-àdica, per tant les úniques completacions possibles són els cossos p-àdics i $\mathbb{R}$. Aquests primers tenen una construcció similar a $\mathbb{R}$ i es poden entendre com successions infinites de nombres racionals i, a part, es poden representar com tires infinites $a_{-m}p^{-m} + ... + a_0 + a_1p + a_2p^2 + ... + a_kp^k + ...$ de nombres enters $a_i \in \mathbb{Z}/p\mathbb{Z}$. Comprovar quan els cossos p-àdics tenen solució en equacions polinòmiques es bastant senzill en relació a comprovar si en tenen en $\mathbb{Q}$ i té una estreta relació amb saber quan en tenen en $\mathbb{Z}/p\mathbb{Z}$ com hem vist en el lema de Hensel.

Les formes quadràtiques ϕ compleixen que representen un element α si i només si $\phi - \alpha Y^2$ és isotròpica i en cossos finits quan tenen més de 3 variables passen a ser isotròpiques, això ens permet saber que a partir de 5 variables tindran solució no-trivial independentment dels coeficients, per tant es redueixen a 5 els casos d'estudi.

Si una forma $aX^2 + bY^2 - Z^2$ es isotròpica en $\mathbb{Q}_p$ ho podem saber amb el símbol de Hilbert, $(a, b)_p$. Si és 1 la forma es isotròpica. Existeix un algoritme finit per computar-lo i a part té unes propietats interessants com el fet de ser multiplicatiu.

Altres variables com l'invariant de Hasse, el determinant resulten ser invariants per equivalències i junt amb la dimensió determinen únicament la forma quadràtica, i també quan una forma és isotròpica o no.

Finalment, en el teorema de Hasse-Minkowski, veiem que una forma quadràtica té solució no trivial en $\mathbb{Q}$ si i només si en té en totes les completacions $\mathbb{Q}_p$ i $\mathbb{R}$. D'això en diem que es compleix el principi local-global en les formes quadràtiques.

Aquest teorema té alguna aplicació com veure que un nombre enter qualsevol pot ser expressat com la suma de 4 o menys quadrats enters o, com veiem després, com la suma de 3 nombres triangulars.

En general el principi local-global no es compleix ja que tenim contraexemples, com el de Selmer, i d'altres que veiem al treball de grau superior.

11 Context Històric

Repassant el contingut matemàtic del treball un s'adona de l'excel·lència matemàtica de Helmut Hasse i de Hermann Minkowski. Amb la seva imaginació van obrir un nou camí en la teoria de nombres, amb la seva ment van sostenir tot el coneixement necessari, per a poc a poc, demostrar el teorema. Juntament, no caldria dir-ho, amb l'ajuda de molts matemàtics que els havien precedit com Kurt Hensel i molts d'altres. Hermann Minkowski, un estudiós des de ben jove, reconegut als 18 anys amb el premi de l'Acadèmia Francesa de la Ciència per el seu treball en formes quadràtiques, va demostrar el teorema per el cos dels racionals. Uns anys més tard Helmut Hasse va generalitzar el teorema i el va demostrar per qualsevol cos. Entre els dos havien concebut el principi local-global i li havien donat un significat. El seus noms passarien lligats a la història de les matemàtiques. Una cosa que segurament, de no haver mort Hermann Minkowski 11 anys abans, no hauria agradat a cap dels dos.
Hermann Minkowski tenia ascendència jueva i Helmut Hasse era un nazi confés.

Hasse va sol·licitar en repetides ocasions l'ingrés al partit Nazi, i finalment va ser acceptada, tot i que en un principi va ser denegada, irònicament, al tenir una àvia jueva. En una conferència a Pisa va afirmar que els polonesos no s'haurien de dedicar a les matemàtiques si no en anar a les mines de carbó o agricultura i en una conferència a la Universitat d'Ohio al 1961, amb 63 anys, va dir que l'esclavitud a América havia sigut una bona institució pels negres.

La vida de Hermann, tot i ser breu, ja que va morir amb 44 anys, denota una vida més alegre. Començant pel fet que va morir el 1909 i no va viure ni veure cap guerra mundial. Va ser un gran amic del matemàtic David Hilbert, qui li va dedicar unes boniques paraules en la seva necrologia:

"Des dels nostres anys d'estudi, Hermann Minkowski va ser el meu millor amic, el qui podia fer més confiança, un amic que em va ajudar en els moments més difícils amb la seva lleialtat i profunditat tant característica. La ciència, la qual estimàvem per sobre de tot, ens va ajuntar per sempre; per a nosaltres semblava un jardí ple de flors. En ell, disfrutàvem buscant camins amagats i descobríem a molta gent noves perspectives que responien al nostre concepte de bellesa, i quan un li ensenyava a l'altre ens meravellàvem junts, la nostra felicitat era completa.Ell va ser per a mi un regal estrany provinent del cel i he d'estar agraït per haver-lo posseït tant temps. Ara la mort se l'ha endut, però el que la mort no es podrà endur mai és la seva noble imatge als nostres cors i tot el coneixement del seu esperit continua actiu en nosaltres."

Metafòricament podríem dir que Helmut Hasse no va saber aplicar el principi local-global, ja que, observant el seu entorn, veiem grans personalitats d'origen jueu. Kurt Hensel va ser el seu professor, un eminent en nombres p-àdics, de fet va ser Hasse qui va escollir ser el seu alumne ja que quan va veure els treballs de Hensel i que aquest donava classe a la universitat de Marburg no va dubtar en inscriure's i ser alumne seu. Kurt Hensel provenia de família jueva, però això no va impedir que tinguessin una relació d'amistat i professional ben estreta. També amb Emmy Noether, reconeguda matemàtica, jueva i companya seva a la universitat de Göttingen van mantenir contacte fins i tot quan ella ja havia emigrat als estats units, i podríem seguir citant personalitats jueves amb qui es va relacionar. Per tant, aquesta bona relació amb les persones jueves del seu entorn

contrasta amb la seva nefasta posició política a favor de la discriminació i repressió, que acabaria portant a l'extermini, del col·lectiu jueu.

Referències

[1] Koblitz, Neal: P-adic numbers, P-adic analysis, and zeta functions, *Springer*, 1984.

[2] Serre, J. P.: A course in arithmetic, *Springer*, New York, 1973.

[3] Bilu, Yuri: p-adic numbers and Diophantine equations, *Fall semester, 2013*.

[4] Cohen, Henry: Number theory: Volume I, Tools and diofantine equations, *Springer*, 2007.

[5] Araújo, Manuel: Classification of quadratic forms, `https://www.math.tecnico.ulisboa.pt/ ggranja/manuel.pdf`, 1 de Juny de 2020.

[6] Lafuente, Ramiro: Los Números p-ádicos y el teorema de Hasse-Minkowski, `http://www.mate.unlp.edu.ar/ demetrio/files/u15/ramiro.pdf`, 3 de Juny de 2020.

[7] Soto, Eduard; El contraexemple de Selmer al principi de Hasse, *Treball final de Grau*, 21 de juny de 2013.

2010 Mathematics Subject Classification. 11-00